Norton Internet Security™ for Macintosh User's Guide

Norton
Internet Security™
For Macintosh

Norton Internet Security™ for Macintosh User's Guide

Copyright Notice

Documentation version 1.0

PN: 07-30-00445

Trademarks

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BEFORE YOU CLICK ON THE "ACCEPT" BUTTON AT THE END OF THIS DOCUMENT, PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH CASE YOU SHOULD CLICK THE "DO NOT ACCEPT" BUTTON, NOT USE THE SOFTWARE AND REMOVE THE SOFTWARE FROM YOUR SYSTEM. BY CLICKING ON THE "ACCEPT" BUTTON, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT.

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

(i) use one copy of the Software on a single computer;
(ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
(iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
(iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
(v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

You may not:

(i) copy the documentation which accompanies the Software;
(ii) sublicense, rent or lease any portion of the Software;
(iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
(iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

¥ Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R. §12.212 and 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd, Cupertino, CA 95014.

General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 20330 Stevens Creek Blvd, Cupertino, CA 95014.

C O N T E N T S

Chapter 3 Protecting disks, files, and data from intrusion

Chapter 4 Responding to access attempts

Chapter 5 Customizing firewall protection

Chapter 6 Troubleshooting

Section 3 Norton AntiVirus for Macintosh

Chapter 7 Protecting disks, files, and data from viruses

Chapter 8 Responding to virus alerts

Appendix A Keeping virus definitions and program files current

Service and support solutions

CD Replacement Form

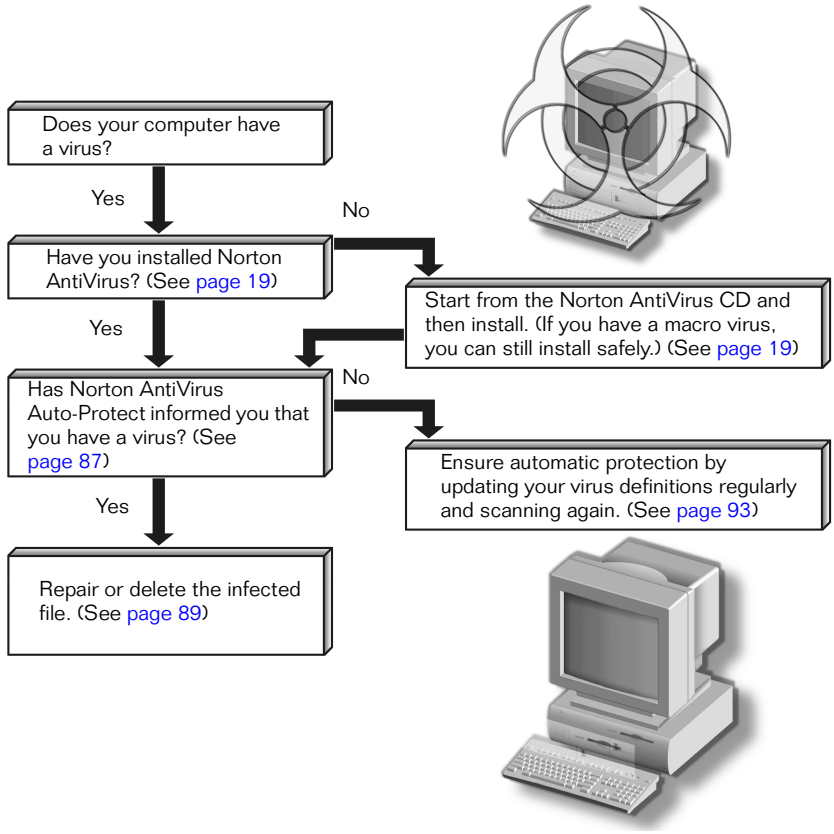
Glossary

Index

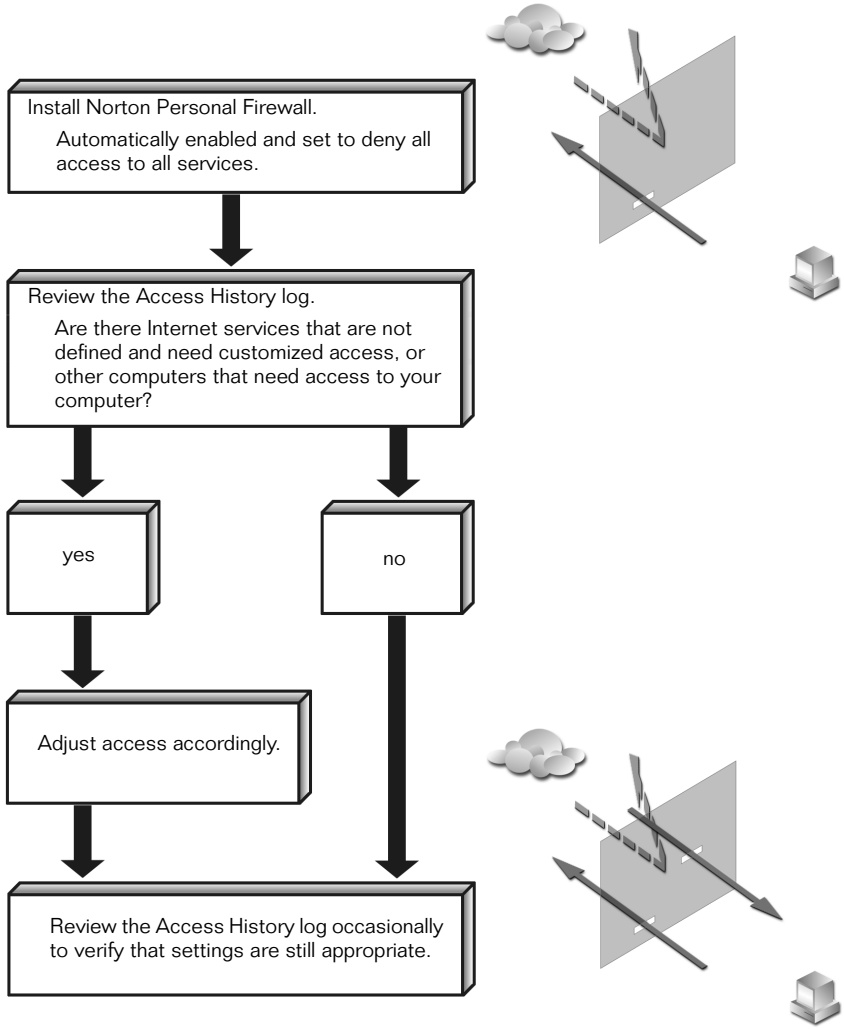
1

Getting Started

What to do if a virus is found



How to use a firewall



CHAPTER 1

Installing Norton Internet Security

Norton Internet Security for Macintosh provides comprehensive virus prevention, detection, and elimination as well as complete intrusion protection for your Macintosh computer.

Norton Internet Security also includes Aladdin iClean, which frees disk space and helps ensure your online privacy by removing unneeded Internet clutter such as cookies, cache files, and logs. Aladdin iClean is installed and documented separately from Norton Internet Security. Documentation for installing and using Aladdin iClean is located in the Aladdin iClean folder on the CD.

System requirements

To use Norton Internet Security, your computer must meet the following minimum requirements:

- Macintosh Power PC processor
- CD-ROM drive
- 24 MB of memory
- 12 MB free disk space
- Internet connection
- Macintosh OS 8.1 or later (8.5 or later for Control Strip functionality)
- Open Transport 1.3 or later

What is a virus?

A *computer virus* is a parasitic program written by an ill-intentioned programmer. Viruses are spread through disks, local networks, and the Internet. Computer viruses attach to programs.

Some viruses, such as *macro viruses*, spread via Microsoft Office files and can be transferred between PCs and Macintosh computers. Macro viruses are not known to damage Macintosh operating systems or hardware, but they can damage Microsoft Office data files and spread whenever you open an infected file.

What are virus definitions?

Virus definitions are files that contain virus footprints that let Norton Internet Security recognize viruses and intercept their activity. You can look up virus names in Norton Internet Security, and access an encyclopedia of virus descriptions on the Symantec Web site. For more information, see "Looking up virus names and definitions" on page 84.

Is my computer protected now?

Norton Internet Security installs both Norton AntiVirus and Norton Personal Firewall when you select Easy Install.

When you have installed Norton AntiVirus using Easy Install, you have complete virus protection. However, new viruses are created constantly. Symantec must create a virus definition for each newly discovered virus, and you must update virus definitions regularly to stay protected. See "How to update virus protection" on page 93 for more information.

Installing Norton Personal Firewall automatically blocks all outside access to your computer. You need only adjust the firewall settings to grant access to those who should have it (if any). See "Protecting disks, files, and data from intrusion" for more information.

Tips for avoiding viruses

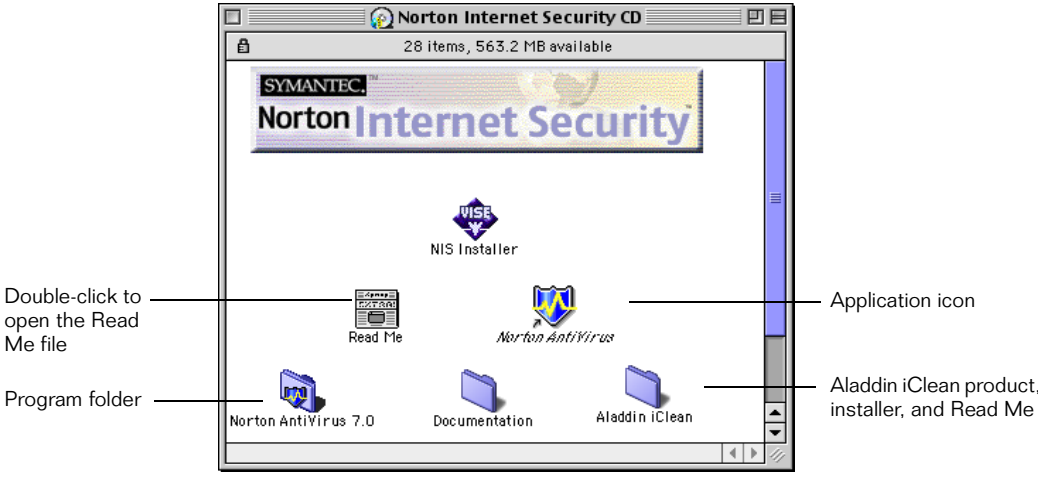
Viruses can spread when you start your computer from an infected disk or when you run an infected program.

To avoid viruses:

- Use LiveUpdate regularly to update your program and virus definitions files. For more information, see "How to update virus protection" on page 93.
- Create a SafeZone for the folder to which you download files. This ensures that Auto-Protect scans all downloaded files. For more information, see "What part of my computer is protected?" on page 75.
- Keep Norton AntiVirus Auto-Protect turned on at all times to prevent viruses from infecting your computer. If Norton AntiVirus Auto-Protect is not turned on, scan disks before you use them.
- Back up files regularly and keep more than just the most recent backup. Also, make a backup copy of your uninfected System folder.
- Write-protect removable media.
- Schedule scans to occur automatically. For more information, see "Scheduling a scan event" on page 82.
- Stay informed about viruses by logging on to the Symantec Web site (http://www.sarc.com) where there is extensive, frequently updated information on viruses and virus protection.

About your Norton Internet Security for Macintosh CD

Use your Norton Internet Security for Macintosh CD to install your software. It contains System software that lets you reboot when you need to scan for viruses.



In addition to the Norton Internet Security for Macintosh Installer, several other items are also on the CD:

- Read Me file: Contains late-breaking information, troubleshooting tips, installation instructions, and the default location of all files installed by Norton Internet Security.
- Documentation folder: Contains the *Norton AntiVirus Reference Guide* and the *Norton Personal Firewall User's Guide* in .pdf format and installation files for Adobe Acrobat Reader.
- System folder: Lets you restart your computer from the CD to run Norton AntiVirus for Macintosh before you install it, or any time you need to scan the disk containing your active System folder.
- SimpleText application: Lets you read the Read Me file.

Installing Norton Internet Security for Macintosh

Restart your computer from the Norton Internet Security CD and scan for viruses before installing. This ensures that no viruses are in memory and that no system extensions cause conflicts during installation.

For late-breaking information and installation troubleshooting tips, see the Read Me file on the CD.

To read the file:

- Insert the CD into your CD-ROM drive and double-click the Read Me file.

Once you have checked the Read Me file, install Norton Internet Security.

Old Norton AntiVirus for Macintosh and Symantec AntiVirus for Macintosh (SAM) files are deleted when you install Norton AntiVirus to the same location. If they are in a different location, delete them.

If you are installing Norton Personal Firewall in the same location as a copy of Open Door's DoorStop firewall, the DoorStop files will be deleted, but your DoorStop settings will be maintained in Norton Personal Firewall.

Starting from the CD

If you suspect that your hard drive is infected by a virus, you can use the Norton Internet Security for Macintosh CD to start your computer and scan before you install.

To start your computer from the Norton Internet Security for Macintosh CD:

1. Insert your Norton Internet Security for Macintosh CD into the CD-ROM drive.
2. Restart your computer from the Norton Internet Security for Macintosh CD by using one of the following methods:
   - On the Special menu, click Restart, while pressing the C key on the keyboard.
   - On a Macintosh computer with a third-party or external CD-ROM drive, go to Control Panels, click Startup Disk, select the Norton Internet Security for Macintosh CD as your Startup Disk. Close the Startup Disk control panel. On the Special menu, click Restart.

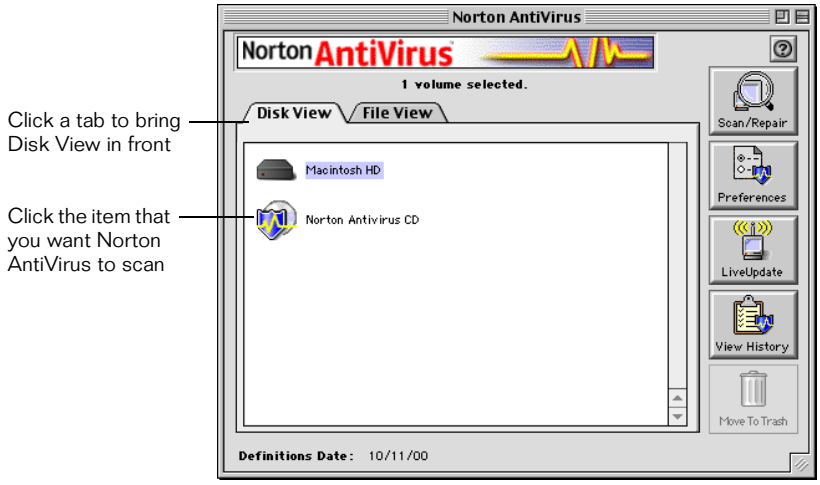
You can tell that your computer has restarted from the CD because the Norton Internet Security for Macintosh pattern appears in the background of the Desktop.

If the CD window doesn't open automatically, double-click the CD icon to open it.

To scan your hard drive:

1 Open Norton AntiVirus.

2 In the Norton AntiVirus main window, select the disk to scan.



3 Click Scan/Repair.

If a virus is found during the scan and auto-repair is turned on, Norton AntiVirus repairs it automatically. If auto-repair is turned off, click Repair to try and repair the infected file.

If the infected file can't be repaired, Norton AntiVirus tells you what to do when you click the infected file. For more information, see "If a virus is found while scanning" on page 89.

4 Click Done to close the Summary window.

5 On the File menu, click Quit or press Command-Q to close the window.

If the Virus Scanning Preferences do not include repairing infected files automatically, the Scan/Repair button name is Scan. For information on Virus Scanning Preferences, see "Selecting a protection level during

installation" on page 24, and "Turning Auto-Protect on or off with the Control Strip" on page 76.

Installing after scanning

After you have restarted your computer from the CD and scanned your system to ensure that it is virus-free, you are ready to install Norton Internet Security for Macintosh.

To install Norton Internet Security for Macintosh:

1. Insert the Norton Internet Security for Macintosh CD into the CD-ROM drive.

   If the CD window doesn't open automatically, double-click the **CD** icon to open it.
2. In the CD window, double-click **NIS Installer**.
3. Follow the prompts to progress through the information screens.

   If you click **Decline** on the License and Warranty Agreement, the installation is cancelled.
4. Do one of the following:
   - For a full installation, click **Easy Install**.
   - To select individual components, click **Custom Install**, and select the components to install.
5. Confirm the destination displayed or specify a different destination folder to which to install.
6. Click **Install**.
7. Read the subscription notice and click **OK**.
8. Select or confirm the Virus Scanning Preferences and click **OK**.

   You can change this at any time after you install. For more information, see "Selecting a protection level during installation" on page 24.
9. Follow the on-screen instructions to complete the installation and click **Restart**.

   The first time you restart your computer after installing Norton Personal Firewall, Norton Personal Firewall opens and displays the status portion of the Setup window to verify that the firewall is

enabled. Quit the program to clear your screen. The firewall remainsenabled.

If you used the Startup Disk Control Panel settings to start your computer from the Norton Internet Security for Macintosh CD, restore the old settings before you restart.

To restore your computer's settings:

1. Go to Control Panels.
2. Click Startup Disk.
3. Click your hard disk to make it the startup disk.
4. Close the Control Panel.
5. On the Special menu, click **Restart**.

If you have trouble ejecting the CD after you restart your computer, try one of the following:

- Press the CD-ROM drive's eject button when your Macintosh restart chime sounds.
- On newer Macintosh computers with a slot-loading CD-ROM drive, press the mouse button while starting up to eject the CD.

When you install Norton Internet Security with the Standard Protection, you are protected from intrusion and most viruses after you restart. With this level of protection, Norton AntiVirus Auto-Protect loads when you restart and actively protects your computer unless you turn Auto-Protect off; Norton Personal Firewall extension also loads and protects your computer unless you disable it.

If you can't start from the Norton Internet Security for Macintosh CD

The System software included on the Norton Internet Security for Macintosh CD might not be sufficient to start newer Macintosh models issued after the release of this version of Norton Internet Security for Macintosh. To find out if a newer CD is available, contact Symantec's Customer Service. For more information, see "Service and support solutions" on page 103.

Some third-party CD drives cannot start a computer from a CD. As an alternative to the CD, set up another hard drive, a partition on a hard drive, or a removable disk such as a Zip or SuperDisk drive as a startup disk.

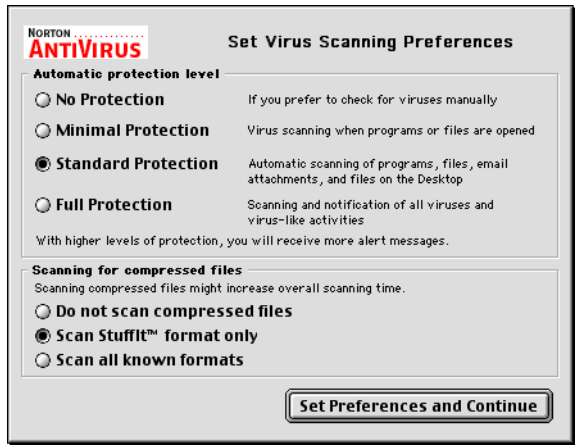
To set up another drive as a startup disk:

1. Install your Macintosh OS System software to the designated drive.
2. Install Norton Internet Security for Macintosh on the new startup disk.
3. Restart your computer from the new startup disk to run Norton Internet Security in an emergency.
4. Use the Startup Disk Control Panel to set it as the startup drive by doing the following:
   - **a** On a Macintosh computer with a third-party or external CD-ROM drive, go to Control Panels.
   - **b** Click Startup Disk.
   - **c** Select the Norton Internet Security for Macintosh CD as your Startup Disk.
   - **d** Close the Startup Disk Control Panel and click Restart on the Special menu. Your computer will start up from the designated volume.

Now you can install Norton Internet Security on your main hard drive.

Selecting a protection level during installation

During the Norton AntiVirus for Macintosh installation process, you can select a level of virus protection that matches your computing needs. These levels are combinations of more detailed custom preferences.



Choose from the following protection levels:

- No Protection: Auto-Protect is turned off. You have no automatic virus protection with this setting. You can scan for viruses manually, use the contextual menu to scan selected items, or use the control-strip feature to turn Auto-Protect on.
- Minimal Protection: Auto-Protect is turned on, but only to scan files that are being opened or created, and Internet file downloads.
- Standard Protection: This setting monitors Internet activity, installations, file exchanges, and provides warnings of common virus-like activities.
- Full Protection: With this setting, all of your computing activities are monitored for virus activities. If you use File Sharing on your computer, or your computer is exposed to viruses, use this setting.

The Compression Scanning options let you select the types of compressed files Norton AntiVirus will scan. Because compressed files take longer to scan, you might want to adjust these settings.

To change settings later, see "Setting general and custom preferences" on page 77.

About your virus subscription

Norton AntiVirus includes a one-year subscription to virus definitions. Updates are made available monthly, or more frequently when necessary.

You can obtain regular virus definitions updates manually or on a customized schedule using LiveUpdate.

For more information, see "About LiveUpdate" on page 93.

What to do after installing

When you restart your computer after installing Norton AntiVirus with Standard protection, Auto-Protect loads into memory, providing constant protection to your computer, including hard disk, memory, and downloads from the Internet or email.

Norton Personal Firewall also loads into memory and is set to block all outside access to your computer. If you do not need to provide access to another computer, you need do nothing more with Norton Personal Firewall. Otherwise, for further information, see "Customizing firewall protection" on page 55.

Update your virus definitions. See "Keeping virus definitions and program files current" on page 93.

Scan your hard disk using the latest virus definitions to make sure there are no recent viruses. See "Scanning for viruses" on page 78.

For more information

Context-sensitive Help is built into both the Norton AntiVirus for Macintosh and the Norton Personal Firewall applications. The *Norton AntiVirus for Macintosh Reference Guide* .pdf file contains additional information about Norton AntiVirus for Macintosh.

To access Help:

- Click **Help** in any window in Norton AntiVirus or Norton Personal Firewall.

Norton Personal Firewall Help appears in a window on your Web browser. Norton AntiVirus Help appears as an Apple Guide.

Norton AntiVirus Balloon Help contains explanations of items on the screen.

To turn on Balloon Help:

- On the Help Menu, click Show Balloons; point to any item to see a description.

The *Norton AntiVirus for Macintosh Reference Guide* and the *Norton Personal Firewall User's Guide* are available in printable Adobe Acrobat .pdf format on the CD. An Adobe Acrobat Reader can also be installed if it is not already on your computer.

Note: The Read Me file on the Norton Internet Security for Macintosh CD contains information that was unavailable at the time this User's Guide was published. Read this information before you go any further.

Accessing the .pdf files

You must have Adobe Acrobat Reader installed to read the *Norton AntiVirus for Macintosh Reference Guide* and the *Norton Personal Firewall User's Guide* .pdf files. If you do not have it installed, install it from the Norton Internet Security for Macintosh CD.

You cannot view the .pdf files if you started your computer from the CD, because Acrobat Reader will not run when you have started from a locked device. To have this documentation available while started from the CD, print it while started normally from the hard drive or from another computer.

To install Adobe Acrobat Reader:

1. In the Norton Internet Security for Macintosh CD window, double-click the Documentation folder.
2. Double-click the Adobe Acrobat Reader installer icon.
3. Follow the prompts to select a folder for Adobe Acrobat Reader and complete the installation.

To open a .pdf file:

1. In the Norton Internet Security for Macintosh CD window, double-click the Documentation folder.
2. Double-click the guide you want to open.

   You can also drag the .pdf file to your hard disk. The *Norton AntiVirus Reference Guide* needs approximately 5 MB of disk space. The *Norton Personal Firewall User's Guide* needs approximately 8 MB of disk space.

Registering Norton Internet Security for Macintosh

Using your existing Internet connection, you can register Norton Internet Security for Macintosh via the *Internet* (the global network of computers).

If you are running Macintosh OS 8.5 or higher, an icon in the Norton Internet Security for Macintosh folder lets you launch your browser and connect to the Symantec software registration page. If you are running an earlier version of Macintosh OS, point your browser to the Symantec Web page.

To register via the Internet:

1. Connect to the Internet.

   If you use America Online (AOL) to connect to the Internet, see "To register your software via AOL:" on page 29.

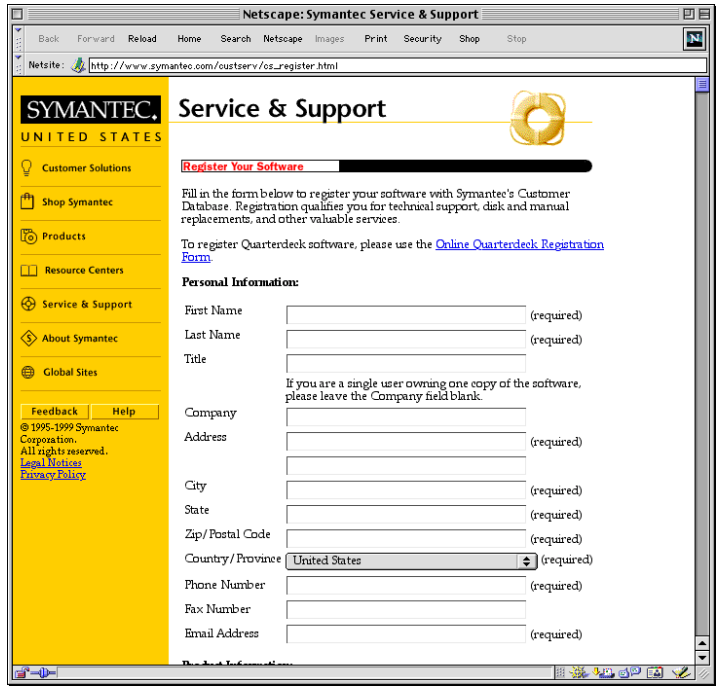
2. In the Norton Internet Security for Macintosh folder, double-click **Register Your Software**.

   Your default Internet browser displays the Symantec Service & Support registration page.

3. If you are using Macintosh OS 8.1, start your browser and navigate to the Symantec Service & Support page:

   www.symantec.com/custserv/cs_register.html

4. On the Service & Support page, type all of the required information.



5. Click **Submit Registration**.

Reading Late Breaking News

Norton Internet Security for Macintosh installs a Late Breaking News link. Use this link to get the latest information available for your installed software.

To read Late Breaking News:

1. Connect to the Internet.

   If you use America Online (AOL) to connect to the Internet, see "To read Late Breaking News via AOL:" on page 30.

2. In the Norton Internet Security for Macintosh folder, double-click **Late Breaking News**.

   Your default Internet browser displays the Symantec Late Breaking News Web page for your product.

3. If you are using Macintosh OS 8.1, start your browser and navigate to the Symantec Web page:

   http://www.symantec.com/product/home-mac.html

Connecting to the Symantec Web site through America Online

If you use America Online (AOL) as your Internet Service Provider (ISP), you must connect to AOL before you go to the Symantec software registration page or view the Late Breaking News.

To register your software via AOL:

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Move the AOL browser and any other open AOL windows out of the way.
4. In the Norton Internet Security window, double-click **Register Your Software**.
5. On the Service & Support page, type all of the required information.
6. Click **Submit Registration**.
7. Disconnect from AOL.

To read Late Breaking News via AOL:

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Move the AOL browser and any other open AOL windows out of the way.
4. In the Norton Internet Security for Macintosh folder, double-click **Late Breaking News**.

   Your browser displays the Symantec Late Breaking News Web page for your product.
5. When you have finished reading, disconnect from AOL.

Uninstalling Norton Internet Security

You must use the Norton Internet Security CD to remove Norton Internet Security from your system.

To uninstall Norton Internet Security:

1. Insert the Norton Internet Security CD into the CD-ROM drive.

   If the CD window doesn't open automatically, double-click the **CD** icon to open it.
2. In the CD window, double-click **NIS Installer**.
3. Click through the information screens to the Install selection screen.
4. From the list, click **Uninstall**.
5. Select the location from which to uninstall Norton Internet Security.
6. Click **Uninstall**.

2

Norton Personal Firewall

CHAPTER 2

About Norton Personal Firewall

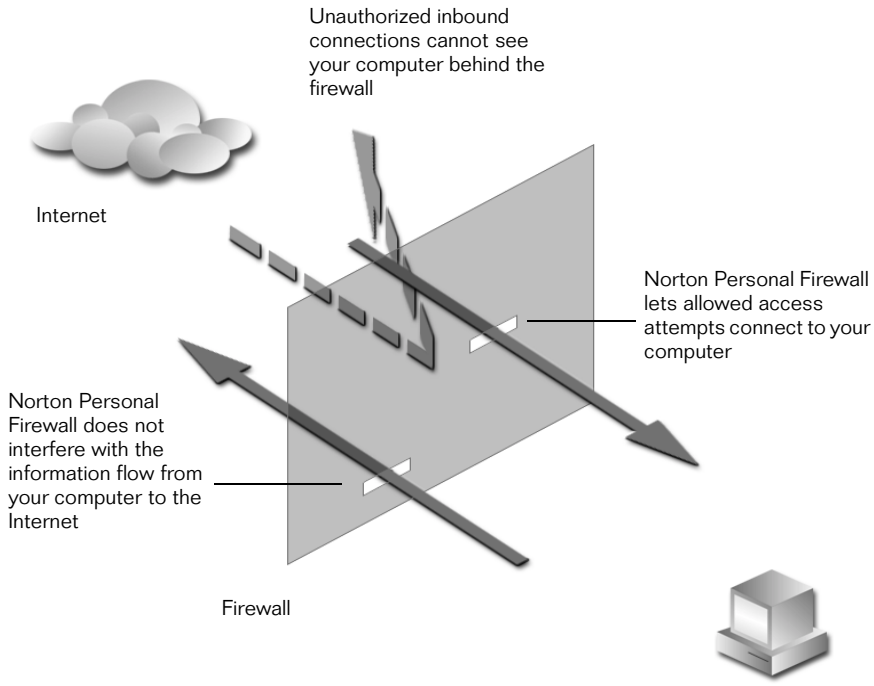
Millions of computers are connected to the Internet, and the number increases daily. When you connect to the Internet, you can connect with millions of other computers. Those computers can also connect with your computer. Unprotected connections to the Internet leave your computer vulnerable to *hacker* attacks, *viruses*, *Trojan horses*, and many other Internet threats. (Hackers are people who break into computers without permission. Viruses and Trojan horses are programs that can corrupt the data on your computer.)

Norton Personal Firewall helps you monitor and control connections to your computer. It helps protect your security and privacy.

How Norton Personal Firewall works

Norton Personal Firewall provides a barrier called a *firewall* between your computer and the Internet. Firewall programs are filters that block or allow connections over the Internet. By filtering connections, firewalls protect your computer from malicious Internet activity.

Norton Personal Firewall uses access settings to determine whether to permit or block connections. You can change these settings, permitting or blocking other computers from accessing your computer.



You specify the services you want to protect (such as Web Sharing or File Sharing) and from which computers. You can allow or deny all access to a particular service, or allow or deny access to a service from certain computers. For example, you can block all access to File Sharing while allowing access to Web Sharing for computers belonging to people you know.

Determining which computers get access

In most cases, you do not need to allow anyone access to your computer. However, there are certain computer configurations and Web and file sharing situations that require you to allow access. For example:

- If you have two or more computers networked, and at least one has Internet access. In this case, every computer with Internet access needs a copy of Norton Personal Firewall installed, with access allowed only to the other computer on the network.

- If you have a Web site on your computer, such as one containing a family photo album, to which you want to restrict access. Using Norton Personal Firewall, specify Web sharing access to those whom you want to see your site, such as other family members.
- If you are using a free Internet service provider, it may require access to a port on your computer to maintain your connection. If the ISP is not granted that access, you lose the service.

When installed, Norton Personal Firewall is set to log all access attempts. You can always check the Access History window to see if someone isn't getting through who should.

For information on using the Access History window, see "Respond to access attempts" on page 49.

What can happen without a firewall

When you are connected to the Internet or another network, others connected to that network can access your computer. This situation can be especially dangerous if you have enabled file sharing or program linking. The danger comes from people commonly known as hackers.

In the programming community, a hacker is someone who enjoys exploring computers and their capabilities; the term carries no negative connotations. Programmers prefer to refer to malicious hackers as *crackers*. However, in the security community, the word cracker refers to someone who cracks code, not necessarily for malicious reasons. As the word hacker is more commonly used outside of the programming community to indicate someone who breaks into computers to cause damage, that is the term used in this book.

Hackers access other people's computers for a variety of reasons:

- To obtain information that can be used for their profit or other advantage.
- To destroy data or otherwise disrupt processing on the computer.
- To prove that they can.

There are as many motives for hacking as there are hackers. Assuming that you are safe because you are anonymous is misguided. Hackers don't necessarily care whose computer is attacked. They just look for one that's unprotected.

CHAPTER 3

Protecting disks, files, and data from intrusion

Norton Personal Firewall protects your computer from connections using the access settings you specify. You can allow access for certain computers, listing them by IP address, and you can define additional services to protect on your computer. Norton Personal Firewall tracks all access attempts and works together with AppleTalk to control access. You can turn Norton Personal Firewall off and on when you need to.

What Norton Personal Firewall protects

Norton Personal Firewall protects your computer from outside intrusion through *TCP/IP* (Transmission Control Protocol/Internet Protocol) and, optionally, *UDP* (User Datagram Protocol) connections. This means that, while you are connected to the Internet or another network, no computer can access the files, programs, or other information on your computer without your authorization. This authorization is granted to a computer, not to an individual user, so any user on that computer has access.

Norton Personal Firewall cannot be used to control outgoing information. For example, you cannot use it to block connections to objectionable Web sites, nor can you use it to encrypt personal information such as a credit card number that you are providing to a Web site. It also does not block direct *AppleTalk* connections (AppleTalk is a communications protocol unique to the Macintosh).

For more information about how Norton Personal Firewall works with AppleTalk, see "Norton Personal Firewall and AppleTalk" on page 39.

Specifying access by IP address

When you allow or deny access for certain computers, you list those computers by their Internet *protocol* (IP) addresses (protocols are sets of rules that govern data transmission). *IP addresses* consist of four numbers from 0 to 255, connected by periods, such as 216.35.137.202. Every computer on the Internet has a unique IP address.

You may not know a computer's IP address, but you know its *host name*. A host name is the name that identifies a computer on a network. For example, www.symantec.com is the host name for the Symantec Web site. Host names are converted to IP addresses by the *Domain Name System (DNS)*. You can enter a host name and search for the IP address using Norton Personal Firewall.

IP addresses can be specified individually, as a range beginning with a certain value, or as a range that corresponds to a *subnet*. A subnet is a local area network that is part of a larger intranet or the Internet.

Defining protection for port numbers

You can list IP addresses to allow or deny access for each service on your computer. The most common services are already defined on the Setup window for you. For those not listed, you can create an entry in the services list by specifying its name and port number.

Internet services communicate by means of ports, with each service using a unique port number. For instance, Web sharing usually uses port 80, and file sharing over TCP/IP uses port 548. Sometimes services are run on alternate ports. If, for example, two *Web servers* (computers that deliver Web pages to your browser) were running on the same computer, they could not both use the same port number—one of them would be assigned an alternate port number. Specifying protection by port number is useful for creating protection for services not predefined by Norton Personal Firewall, and for creating protection for services that use alternate port numbers.

You can also specify protection for services that use UDP ports. However, this feature is intended for use only by those who understand Internet protocols well, as denying access to the wrong UDP ports can prevent your computer from functioning correctly on the Internet.

Tracking access attempts

Norton Personal Firewall records complete information about access attempts to your computer. It can log all denied accesses, allowed accesses, or both, and can provide you with immediate notification of allowed or denied accesses if you so choose.

Norton Personal Firewall and AppleTalk

There are two principal network protocols used on Macintosh computers, AppleTalk and TCP/IP. In general, AppleTalk provides local services that are not available over the Internet such as printing, sharing files with other computers on the same network, and company-specific applications. TCP/IP provides more global services, including such Internet services as email and access to Web sites. With Macintosh OS 9, TCP/IP also provides services that have been traditionally available only over AppleTalk, including file sharing and program linking over the Internet or an intranet.

Users and Groups

The Users and Groups file is the major network security component built into the Macintosh operating system. The Users and Groups file (accessed through either the Users and Groups Control Panel, or in Macintosh OS 9, the File Sharing Control Panel) lets a computer's owner set up user accounts and passwords for access to the computer's built-in network services, and to specify which accounts should have access to which services. User accounts are used to limit access to these services through either AppleTalk or TCP/IP. Access to Guests (users without passwords) can also be specified. Services that use Users and Groups security include Program Linking, File Sharing, Web Sharing, and Remote Access (which lets users dial into a particular computer). Access to these services is often configured through their respective Control Panels.

TCP/IP security on Norton Personal Firewall

Norton Personal Firewall adds a level of protection to any application that uses the TCP protocol by granting access only for limited sets of computers on the Internet, based on their IP addresses. This security is therefore independent of the passwords required by Users and Groups. For example, if you have enabled file sharing over TCP/IP, the file sharing passwords created in Users and Groups will not be enough for the users to gain

access. You must also grant file sharing access for their computers in Norton Personal Firewall. You can either allow all access in Norton Personal Firewall and rely only on the Users and Groups security, or you can allow access only for certain IP addresses, providing two security checkpoints for file sharing access attempts.

AppleTalk and the Internet

When you start Norton Personal Firewall, it warns you if your AppleTalk is using the same port as your Internet connection. If both connections use the same port, it may result in allowing access to your computer over the Internet. If you receive this warning, you should do one of the following:

- Turn off Guest access in Users and Groups.
- Disable AppleTalk while you are connected to the Internet, as Norton Personal Firewall does not protect AppleTalk connections.
- If you are using a product, such as Timbuktu, that provides computer-to-computer access over AppleTalk or TCP/IP, consider disabling the AppleTalk features of the product, as they are not protected by Norton Personal Firewall.

Enabling and disabling firewall protection

When Norton Personal Firewall is installed, it is set to deny access to all TCP/IP services. For most users, these settings provide the protection they need without interfering with their work on the computer. Unless you have specific access rules that you want to define, do nothing after installing Norton Personal Firewall.

You can stop protection at any time by disabling Norton Personal Firewall. For example, you may want to disable Norton Personal Firewall temporarily if you are using *FTP* (File Transfer Protocol). You can disable it for a specified period or until you restart it.

You can disable (or enable) Norton Personal Firewall from two places: the Setup window or the Control Strip (if you have Macintosh OS 8.5 or later).

To disable or enable Norton Personal Firewall from the Setup window:

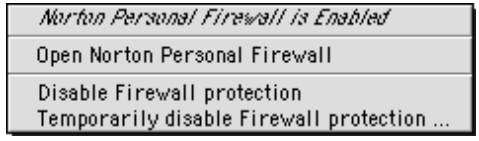
1. Start Norton Personal Firewall by double-clicking the **Norton Personal Firewall** icon.
2. Click **Disable Protection**.

   If Norton Personal Firewall is already turned off, the button reads Enable and can be used to turn on Norton Personal Firewall protection.
3. You will be asked to verify that you want to disable Norton Personal Firewall.
4. Close Norton Personal Firewall.

To disable or enable Norton Personal Firewall from the Control Strip:

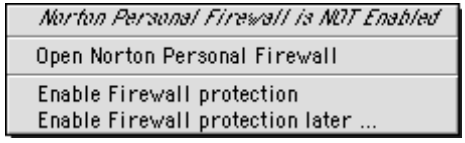
1. Click the Norton Personal Firewall module to open the Control Strip menu.

   Norton Personal Firewall's current status appears as the first line of the menu.



2. Click **Disable Firewall protection** to turn off protection.

   If Norton Personal Firewall is already turned off, the option reads Enable Firewall protection.
3. You will be asked to verify that you want to disable Norton Personal Firewall.



You can also use the Control Strip menu to launch Norton Personal Firewall and to disable protection for a specified time period or enable it after a specified time period.

To disable and enable Norton Personal Firewall after a specified time period:

1. Click the Norton Personal Firewall module to open the Control Strip menu.
2. Click **Temporarily disable Firewall protection** or **Enable Firewall protection later**.
3. Enter the number of minutes after which Norton Personal Firewall is to start.
4. Click **OK**.

About Basic and Advanced modes

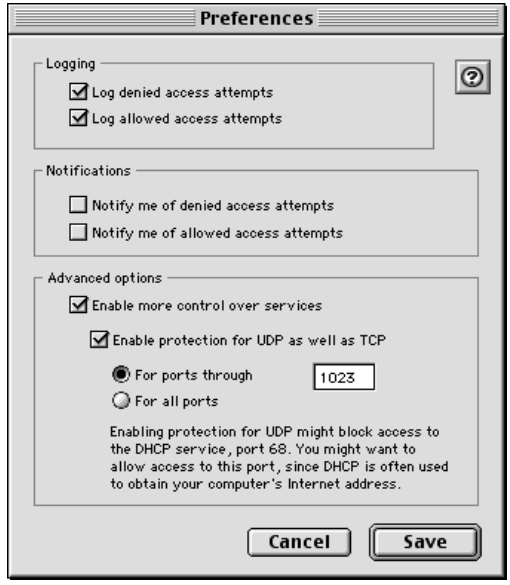
Norton Personal Firewall has two modes of operation: Basic and Advanced. Basic mode is used to define access to the most commonly used services. Norton Personal Firewall is set to Basic mode by default.

Advanced mode is used when you need to:

- Define access settings for a service not already listed in Norton Personal Firewall.
- Specify a subnet other than your own in a list of IP addresses.
- Extend protection to UDP ports.
- See more information about access attempts.

To change to Advanced mode:

1 On the Edit menu, click **Preferences**.



2 Check **Enable more control over services**.

3 Click **Save**.

CHAPTER 4

Responding to access attempts

It's not always easy to tell that Norton Personal Firewall is doing its job—you continue to use your computer as you always have and notice no difference. This is exactly how it's supposed to work. The firewall is in place, blocking any unwanted intrusions.

Norton Personal Firewall logs all access attempts, whether they are allowed or denied. Use this log to verify that Norton Personal Firewall is working correctly.

Monitor firewall activity

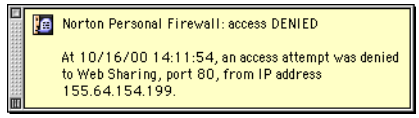
When Norton Personal Firewall is installed, it is set to log both denied and allowed access attempts. These attempts appear in the Access History window, which you can review at any time.

You may want immediate notification of access attempts under certain circumstances. For example, when you first install Norton Personal Firewall, you may want to immediately evaluate every access attempt to ensure that Norton Personal Firewall is working. You may also want to receive immediate notification if you have changed some settings and want to make sure that they have produced the desired results.

To verify protection settings or changes to those settings before going online, use the Norton Personal Firewall self-test feature. Self-test simulates a TCP connection, logs an access attempt, and triggers a notification if you have enabled that feature.

Enable or disable notification of access attempts

You can choose to be notified of all denied access attempts, all allowed access attempts, or both. If you have enabled notification, an alert appears every time an access attempt of the kind specified occurs.



For a description of what to do when you receive an alert, see "Information about alert messages" on page 49.

Enabling or disabling notification has no effect on logging. Also, disabling logging has no effect on notification, although the notification alert will be your only record of the access attempt.

To enable or disable access notification:

1. Double-click the **Norton Personal Firewall** icon or, on the Control Strip menu, click **Open Norton Personal Firewall** to start Norton Personal Firewall.
2. On the Edit menu, click **Preferences**.
3. Specify Notifications options.
4. Click **Save**.

Test firewall settings

Self-test checks firewall protection by simulating access to a service. You can run a self-test in either Basic or Advanced mode. Before beginning, make sure that logging is enabled.

In Basic mode, you can test the services listed in the Setup window, both predefined and custom. The test uses the IP address of your computer. If your computer uses a *PPP* (Point-to-Point protocol) connection and is not currently connected, or if your computer does not have an IP address, self-test uses the IP address 127.0.0.1.

In Advanced mode, you can test an expanded list of services and specify an IP address other than your computer's to use in the test. You may want to enter an IP address that you have listed to be denied access, for example.

To see the results of the self-test, review the Access History window. If you have notification enabled for the type of access attempt being tested, the self-test results in an alert. If Norton Personal Firewall is not enabled, access is allowed to all services and the self-test reflects that.

To use self-test in Basic mode:

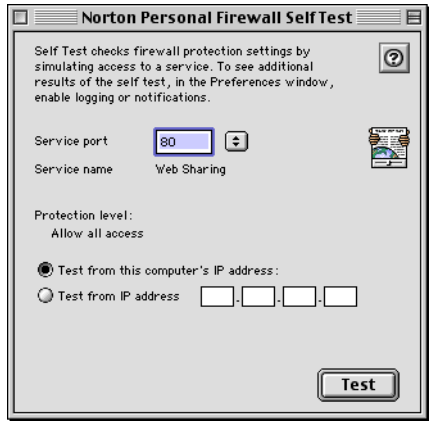
1. Double-click the **Norton Personal Firewall** icon or, on the Control Strip menu, click **Open Norton Personal Firewall** to start Norton Personal Firewall.
2. On the Windows menu, click **Self Test**.

3. Select a service port.

   The protection defined for the chosen service appears under the service name.
4. Click **Test**.

To use self-test in Advanced mode:

1 On the Windows menu, click **Self Test**.



2 Specify a service port number.

The protection defined for the chosen service appears under the service name.

3 Select whether you want to use your computer's IP address or an IP address you specify for the test.

If your computer does not have an IP address, Test from this machine's IP address will be dimmed.

4 Enter an IP address, if applicable.

5 Click **Test**.

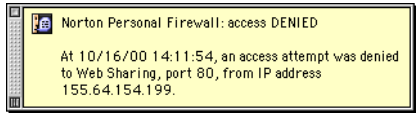
In both Basic and Advanced mode, only TCP services are tested. Protection for a specific UDP service may or may not be the same as the corresponding TCP service, depending on how you have configured Norton Personal Firewall.

Respond to access attempts

View the Access History window occasionally to check for any unusual activity or problem such as denied access for someone who should have access.

Information about alert messages

If you have enabled notification of access attempts, alert messages appear on your screen when access attempts occur.



The alert contains details of the access attempt. If the access attempt seems suspicious, consult the Access History window. For further information on the access attempt in the Access History window, double-click its line.

Notification of further access attempts do not occur until the current notification alert is closed. Also, with operating systems earlier than OS 9, processing in other applications may be suspended until the alert is closed. Do not have notification on with those operating systems if other applications are active and you are away from your computer.

Review Access History

All logged access attempts appear in the Access History window. Use this log of access attempts to spot potential security violations. When reading it, check for patterns such as:

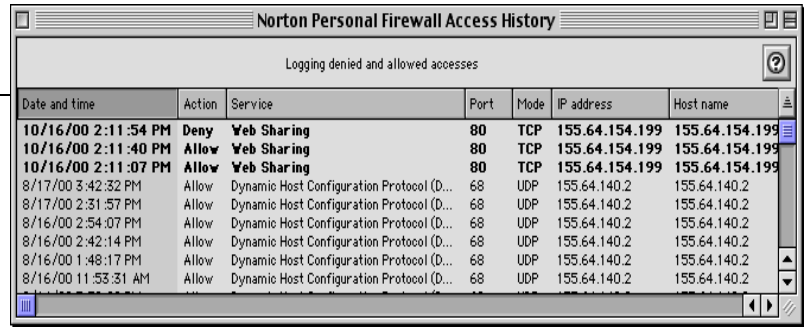
- Many denied accesses, especially from a common client IP address.
- Sequences of port numbers from the same client IP address, possibly indicating a port scan (someone trying many ports on your computer, looking for one that they can access).

It is normal to see some denied access attempts on a random basis (not all from the same IP address, and not to a sequence of port numbers). In some cases, access attempts are made due to activity on your own computer such as connecting to an FTP server and sending email.

To see the Access History window:

1. Double-click the **Norton Personal Firewall** icon or, on the Control Strip menu, click **Open Norton Personal Firewall** to start Norton Personal Firewall.
2. On the Windows menu, click **Access History**.

Advanced mode format



You can view the Access History window in either Basic or Advanced mode. In Basic mode, the Port, Mode, and IP Address columns are not included.

For instructions on changing to Advanced mode, see "To change to Advanced mode:" on page 43.

The type of accesses being logged appears at the top of the window. The fields included in the window are as follows.

Date & Time	The date and time of the access attempt
Action	Whether the access attempt was allowed or denied
Service	The name, if any, of the Internet service to which access was attempted
Port	The port number to which access was attempted
Mode	The protocol used, either TCP or UDP
IP Address	The IP address of the computer from which access was attempted
Host Name	The host name of the computer from which access was attempted

Lines in bold type are less than 15 minutes old.

Sorting columns

By default, lines are sorted by date, with the most recent lines on top.

To sort by other columns:

- Click the column header.

  The header in dark gray is the one currently used for sorting.

Change the sort direction (ascending or descending) by clicking the sorting triangle to the right of the column headers.

Exporting Access History information

The contents of the Access History window can be exported to a tab-delimited text file. The Access History window must be open to export it.

To export the Access History information:

1. On the File menu, click **Export** while the Access History window is open.
2. In the Export dialog box, specify a location for the file and enter a file name.

   To create a new folder for the file, click **New**.
3. Click **Save**.

Clearing the Access History window

If the list in the Access History window gets too long, you can clear the window.

To clear the Access History window:

- On the Edit menu, click **Clear Access History** while the Access History window is open.

  This has no effect on the log file; it still contains the access attempts logged to date.

Learn more about a specific access attempt

You can get more information on any entry in the Access History window.

To open the Access Information dialog box:

- On the Access History window, double-click a line, or select the line and, on the Edit menu, click **Get Info**.

To copy the information to the Clipboard for use by another application:

- In the Access Information dialog box, click **Copy**.

Accessing the Learn More Web site

The Norton Personal Firewall Learn More Web site displays more details about the access attempt and provides links to other sites that may provide details about the source (the Host Name field) of access attempts.

To open Norton Personal Firewall's Learn More Web site:

- In the Access Information dialog box, click **Learn More**.

Change logging preferences

Logging of all access attempts is enabled by default. Keep this setting until you feel confident that your configuration of Norton Personal Firewall is working as you planned. Logging all accesses can create a large log file quickly, so you may eventually want to limit what is being logged.

To change what is being logged:

1. Double-click the **Norton Personal Firewall** icon or, on the Control Strip menu, click **Open Norton Personal Firewall** to start Norton Personal Firewall.
2. On the Edit menu, click **Preferences**.
3. Specify Logging options.
4. Click **Save**.

Disable logging

Logging and service protection are independent of one another. For example, if you are logging allowed accesses and then make Norton Personal Firewall inactive, Norton Personal Firewall will continue logging and will log all accesses, since all accesses are allowed. Under certain circumstances, such as when you want to create a new log file, you will need to disable logging altogether. Disabling logging has no effect on Norton Personal Firewall protection.

To disable logging:

1. Double-click the **Norton Personal Firewall** icon or, on the Control Strip menu, click **Open Norton Personal Firewall** to start Norton Personal Firewall.
2. On the Edit menu, click **Preferences**.
3. Uncheck both Logging options.
4. Click **Save**.

How the log file is structured

The log file is a tab-delimited text file named Norton Personal Firewall Log, located in the Preferences folder on your computer. It is written in an extended WebSTAR log format, which can be read by any word processor or spreadsheet application, or by some log-analyzer applications.

Access attempts are logged using the following tokens (which are included in the !!LOG_FORMAT line whenever Norton Personal Firewall starts or a new log file is written):

DATE, TIME	Date and time of access in WebSTAR standard format
RESULT	OK for an allowed access; ERR! for a denied access
HOSTNAME	IP address of the client attempting access to the given port
SERVER_PORT	The port to which access is attempted by the given client
METHOD	The protocol used by the access attempt (TCP or UDP)

Exporting the log file to a spreadsheet and sorting the data may make it easier to spot patterns that could indicate a potential security violation. For example:

- Sort by the RESULT field and then by HOSTNAME. In the rows containing ERR! in the RESULT field, look for groupings of IP addresses in the HOSTNAME field. Large numbers of ERR! lines for a given IP address may indicate an attempted security breach.
- Sort by RESULT, then by HOSTNAME, and then SERVER_PORT. In the rows containing ERR! in the RESULT field, look for sequences of port numbers in the SERVER_PORT field that have the same IP address in the HOSTNAME field. Sequences of port numbers from a given IP address may indicate a port scan.

For more information on an IP address in the log file (or in a notification alert), refer to the Access History window. For more information on reviewing the Access History window, see "To see the Access History window:" on page 50.

C H A P T E R 5

Customizing firewall protection

As you work with Norton Personal Firewall, you may need to adjust your access settings. For example, you may want to allow file sharing for a colleague working at another location. You may also find a service on your computer that is not listed separately on the Setup window and requires customized protection. You can add that service to the list. You can also extend protection to your computer's UDP ports.

Changes to access settings do not affect computers that are connected to your computer when you make the changes. When the connection is broken, the changes will take effect. For example, if a computer is connected to file sharing on your computer and you deny file sharing access, the computer remains connected until either the user logs off or you explicitly break the connection.

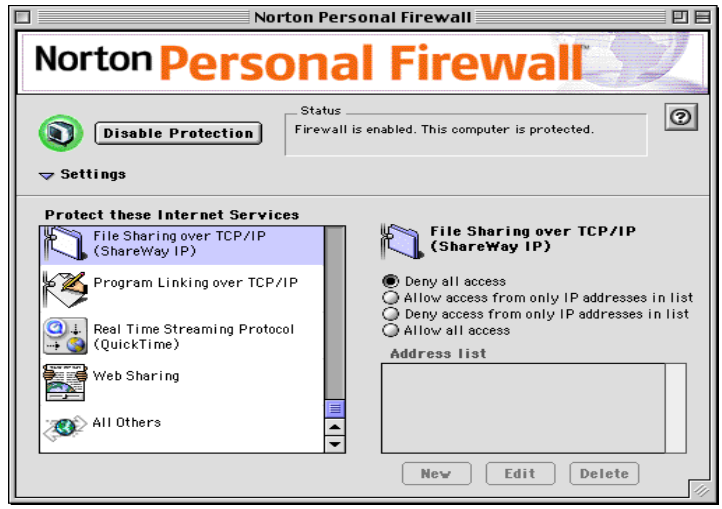
Set protection for standard Internet services

The Internet services built into the Macintosh OS are already defined on the Setup window of Norton Personal Firewall. Services that are not listed are protected using the settings for the All Others service entry. They are all set to deny all access by default. You can change protection settings for any of the services listed.

To open the Setup window:

1. Double-click the **Norton Personal Firewall** icon or, on the Control Strip menu, click **Open Norton Personal Firewall** to start Norton Personal Firewall.
2. If the Setup window does not appear, on the Windows menu, click **Setup**.

3 If you cannot see the entire Setup window, click **Settings** to enlarge it.



The first time you open the Setup window, the protection settings on the right side of the window do not appear. To see the settings for one of the services listed on the left side of the window, click it.

For every service listed in the Setup window, you can:

- Deny all access.
- Allow access to addresses in list.
- Deny access to addresses in list.
- Allow all access.

These settings are listed in order from most restrictive to least restrictive. To deny or allow all access to a service, click the service, then click the option you want.

To allow or deny access to a list of IP addresses, click the service, click the option, and then define the IP addresses to go on the list.

To define a list of addresses to which to allow or deny access:

1 Select the Internet service for which you want to define access.

2 Select whether you want to allow or deny access for a list of IP addresses.

3 Click **New** to add an address or range of addresses to the list.

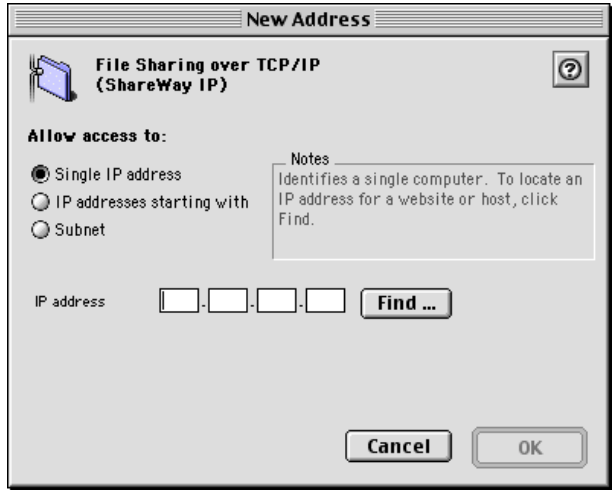
The New Address dialog box appears.

Add IP addresses

Use the first two options in the New Address dialog box to add a single address or range of addresses to the allow or deny access list.

To add a single address:

1 In the New Address dialog box, click **Single IP address**.

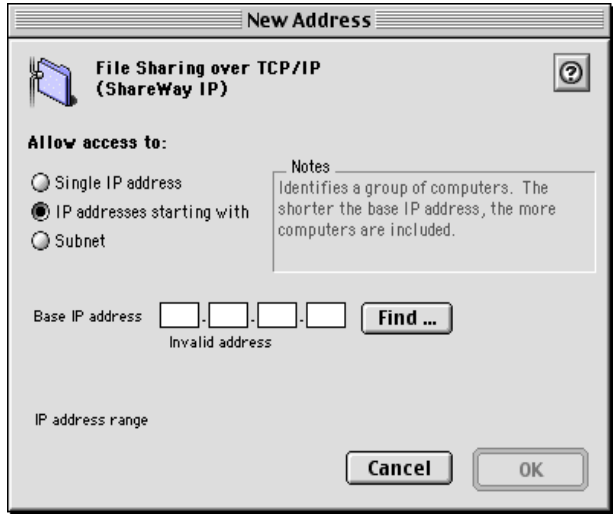


2 In the IP address field, enter the address.

3 Click **OK**.

To add a range of addresses:

1 In the New Address dialog box, click **IP Addresses starting with**.



2 Enter enough of an address in the Base IP address field to get the range of addresses you want.

As you enter each digit of a Base IP address, Norton Personal Firewall determines the end of the range and displays it in the area of the New Address dialog box marked IP address range.

3 Click **OK**.

Search for IP addresses

If you are entering either a single address or a range of addresses, you can search for an address if you know the host name.

To search for an address:

1 In the New Address dialog box, click **Find**.

2 In the Find IP Address dialog box, type the host name.

3 Click **Find**.

4 Click **OK** to enter the IP address found into the address field of the New Address dialog box.

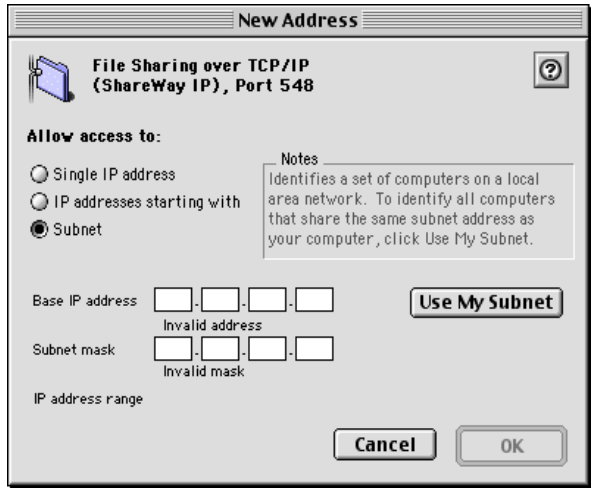
Add subnet addresses

You can add subnets to your deny or allow access list. In Basic mode, you can specify only your own subnet. In Advanced mode, you can specify either your own subnet or a different subnet.

For instructions on changing to Advanced mode, see "To change to Advanced mode:" on page 43.

To add addresses for your own subnet:

1 In the New Address dialog box, click **Subnet**.



2 Click **Use My Subnet**.

The base IP address and *subnet mask* for your subnet are filled in automatically. A subnet mask defines how much of an IP address identifies the subnet.

3 Click **OK**.

To add addresses for a subnet other than your own:

1 In the New Address dialog box, click **Subnet**.

2 Enter the base IP address and the subnet mask for the subnet into the appropriate fields.

3 To use the values for your own subnet, click **Use My Subnet**.

Norton Personal Firewall enters them automatically.

4 Click **OK**.

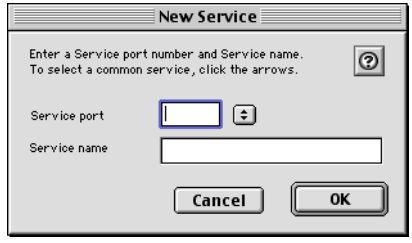
Define a custom service to protect

To specify access for a service that is not listed on the Setup window, you must define that service in Norton Personal Firewall. You must be in Advanced mode to perform this task.

For information on changing to Advanced mode, see "To change to Advanced mode:" on page 43.

To define a new service:

1 On the services list, click **New**.



2 Specify a service port number.

3 Type the name of the service.

If you have selected a port number from the list, the name of the service appears automatically.

An icon for the service appears automatically.

4 You can change the icon by copying and pasting the desired icon over the icon in the New Service dialog box.

5 Click **OK**.

The new service appears in the list on the Setup window. You can now specify access for that service.

For more information, see "Set protection for standard Internet services" on page 55.

Change or delete a custom service

You cannot edit or delete a predefined service, but you can edit or delete a custom service that you added to the list.

To edit a custom service:

1. In the Setup window, select the service.
2. Click **Edit**.
3. In the Edit Service dialog box, change the name of the service or change its icon (by cutting and pasting a new one).
4. To change the port number, delete the service and add a new one with the correct port number.
5. Click **OK**.

To delete a custom service:

1. In the Setup window, select the service.
2. Click **Delete**.
3. In the Warning box that appears, click **Delete** to verify that you want to delete the service.

Change protection settings

You can make changes to the protection settings for a service at two levels. You can change the level of restriction (for example, from "Deny all access" to "Allow access from only addresses in list") or you can change the list of addresses associated with a restriction level. You make these changes in the Setup window.

Change the level of restriction

You can change the level of restriction for a service at any time.

To change the level of restriction:

1. In the Setup window, select the service.
2. Click the new restriction option:
   - If you are changing to a restriction option that refers to a list of IP addresses, you must create that list.

For information on creating a list of IP addresses, see "Set protection for standard Internet services" on page 55.

- If you are changing to either Deny all access or Allow all access from an option with a list of IP addresses, you do not need to delete those addresses. They will remain visible, but dimmed in the Setup window.

Change an IP address list

For either restriction option requiring an address list, you can add to the list, edit the addresses on the list, or delete addresses from the list on the Setup window.

Before changing a list, make sure that the list you want to change is displayed by clicking the appropriate service.

To add to a list:

1. In the Setup window, click **New**.
2. Add IP addresses as necessary.
3. Click **OK**.

For more information on adding IP addresses, see "Add IP addresses" on page 57. For more information on adding subnet addresses, see "Add subnet addresses" on page 59.

To edit an address or range of addresses in a list:

1. In the Setup window, select the address or range.
2. Click **Edit**.
3. In the Edit Address dialog box, make the changes you want.
4. Click **OK**.

To delete an address or range of addresses from a list:

1. In the Setup window, select the address or range.
2. Click **Delete**.
3. In the Warning box that appears, click **Delete** to verify your request.

Set up UDP protection

User Datagram Protocol (UDP) is a relatively simple protocol used for Internet operations. For example, the Domain Name System (DNS), which translates host names into IP addresses, uses UDP.

There is little reason to protect UDP ports. However, you may have a specific reason for protecting a UDP port. Protect these ports with caution, as denying access to UDP services can cause problems when accessing the Internet.

In most cases, you will want to protect only UDP ports up through 1023. These low-numbered UDP ports are used for standard services such as *DHCP* (Dynamic Host Configuration Protocol, commonly used to obtain a computer's IP address) and NTP (Network Time Protocol, which can be used by the Date & Time Control Panel). Higher-numbered ports are used dynamically by certain UDP services such as DNS. Denying access to high-numbered ports disables such services, since there is no way to know which port will be used by a given service.

To enable UDP protection:

1. Double-click the **Norton Personal Firewall** icon or, on the Control Strip menu, click **Open Norton Personal Firewall** to start Norton Personal Firewall.
2. On the Edit menu, click **Preferences**.
3. Check **Enable more controls over services**.
4. Check **Enable protection for UDP as well as TCP**.
5. Specify the range of ports to protect.
6. Click **Save**.

How UDP protection works

Once you enable UDP protection, it works much like TCP protection. Norton Personal Firewall uses the same service list for UDP as it does for TCP. Normally, a service uses either a TCP or a UDP port, but Norton Personal Firewall protects both types of ports for a given service (if UDP protection for that port is active).

One way that UDP protection differs from TCP protection is that UDP is a *connectionless protocol* (does not require a connection to send a message), while TCP is a *connection-based protocol* (requires a connection before

sending messages). With TCP, Norton Personal Firewall can allow or deny only the connection attempt, and not the information following the attempt. With UDP, Norton Personal Firewall must allow or deny every piece of information destined for a particular service. Therefore, it cannot block only incoming connection attempts; it must block all communications associated with the service.

Additional differences with UDP relate to logging and notification. With TCP, even if no service is active on a particular port, Norton Personal Firewall is notified of access attempts to that port and can log those access attempts. In general, Norton Personal Firewall is not notified of access attempts to UDP ports that are not active. It will not log or notify on these attempts, nor will the attempts be included in the Access History window.

Since UDP is connectionless, Norton Personal Firewall logs and notifies on every UDP packet for active ports that it is protecting (if the appropriate options have been configured). You may not want to log allowed accesses if you have enabled UDP protection, due to the number of log entries that could be generated. For example, since DNS uses a UDP port, the log would contain an entry for every time you connected to a Web site.

Even if you only protect lower-numbered UDP ports, you should create specific entries for certain services. For example, if your computer uses DHCP to get its IP address, you may want to specify Allow all (or Allow from addresses in list and enter the DHCP server's IP address) for the DHCP service, port 68. An entry for this service is automatically created by Norton Personal Firewall when you enable UDP protection. For maximum security, access to this service is initially set to Deny all.

CHAPTER 6

Troubleshooting

Frequently asked questions

How do I turn off firewall protection?

You can turn off firewall protection in two places: the Setup window and the Control Strip menu (on Macintosh OS 8.5 or later).

To turn off firewall protection on the Setup window:

1. Double-click the **Norton Personal Firewall** icon.
2. If the Setup window does not appear, on the Windows menu, click **Setup**.
3. Click **Disable Protection**.

To turn off firewall protection on the Control Strip menu:

1. On the Control Strip, click the **Norton Personal Firewall** module to open the menu.
2. Click **Disable Firewall protection**.

You can also use the Control Strip menu to stop Norton Personal Firewall protection for a specified amount of time.

To disable Norton Personal Firewall for a set amount of time:

1. On the Control Strip, click the **Norton Personal Firewall** module to open the menu.
2. Click **Temporarily disable Firewall protection**.
3. Type the number of minutes after which Norton Personal Firewall protection should restart.
4. Click **OK**.

Why can't I download files from a Web site?

You may be using FTP to transfer your files. Many features of the FTP protocol work by having the FTP server open a TCP connection back to your computer and then use that connection as a data port to get data from your computer. The problem is that the port number used for the data port is usually picked at random, which makes it difficult to allow access to the FTP server ahead of time.

To resolve FTP problems, do one of the following:

- On the Control Strip menu, click **Temporarily disable Firewall protection**.

  Norton Personal Firewall needs to be off only when a file transfer begins. If you are transferring several files at once, make sure that Norton Personal Firewall stays off until the last file starts downloading. If you are using a computer with Macintosh OS 8.1, on the Setup window, disable and enable Norton Personal Firewall.
- In the All others service entry, allow access from the FTP server (use the IP address from the Access History window).
- If your FTP client application lets you specify a data port, create a service entry for the port you want to use and allow access for the FTP server.
- If your FTP client application allows the use of passive mode FTP, which does not require a data port, use it. Make sure the Internet control panel (on Macintosh OS 8.5 and later) is set for passive mode (on the Advanced tab).

Why can't I access any Web site?

You have probably enabled UDP protection and have affected a low-level service that your computer needs to perform day-to-day Internet activities. Possibilities include:

- DHCP: Check the TCP/IP control panel to see if your computer is configured to get its IP address using DHCP. If it is, Norton Personal Firewall has created a service entry for DHCP. Edit that service entry to allow the DHCP server access to your computer. Use the DHCP server's IP address from the Access History window.
- DNS: Almost all outgoing Internet operations require DNS, which converts host names to IP addresses. Make sure that you are not blocking the dynamic ports used by DNS (usually ports 32768 or higher).

For information on how to check port numbers that are being blocked, see "Review Access History" on page 49. For information on how to edit a service entry to allow access, see "Add IP addresses" on page 57.

Why doesn't my FTP server work?

If you are running an FTP server on your computer, some clients may have trouble connecting to the server, even though you have allowed access to port 21. If a client is using FTP passive mode, the client may dynamically open a second connection to the server for a data port. Either have the client not use passive mode, or give the client access to the new port being opened by the server.

For information on granting access to a port, see "Define a custom service to protect" on page 60.

Why doesn't my printer work?

You may have turned off AppleTalk in response to the warning that it was using the same port as your Internet connection. Turn AppleTalk back on in order to print.

What service does this port number represent?

Following are TCP and UDP port numbers commonly used by Macintosh services.

TCP port numbers

Port	Usage	Notes
20	FTP data	Used only as a source port
21	FTP control	
23	Telnet	Common port for attacks
25	SMTP (email)	
53	DNS	Mainly uses UDP, not TCP
70	Gopher	
79	Finger	

Port	Usage	Notes
80	HTTP (Web)	
88	Kerberos	
105	PH (directory)	
106	Poppass (change password)	
110	POP3 (email)	
111	Remote procedure call (RPC)	Used for Java
113	AUTH	
119	NNTP (news)	
139	NETBIOS session	Windows access (ASIP 6)
143	IMAP (new email)	
311	AppleShare Web Admin	ASIP 6.1 and later
384	ARNS (tunneling)	
387	AURP (tunneling)	
389	LDAP (directory)	
407	Timbuktu 5.2 or later	Previous versions use other ports
427	SLP (service location)	Only uses TCP for large responses
443	SSL (HTTPS)	
497	Retrospect	UDP for finding clients
510	FirstClass server	
515	LPR (printing)	
548	AFP (AppleShare)	
554	RTSP (QuickTime server)	Also uses UDP 6970+
591	FileMaker Pro Web	Recommended alternate to 80
626	IMAP Admin	Apple extension in ASIP 6
660	ASIP Remote Admin	ASIP 6.3 and later
666	Now contact server	Violates actual port assignment

Port	Usage	Notes
687	ASIP shared U&G port	ASIP 6.2 and later
1080	WebSTAR Admin	WebSTAR port number plus 1000
1417	Timbuktu Control (pre-5.2)	Logon is through UDP Port 407
1418	Timbuktu Observe (pre-5.2)	Logon is through UDP Port 407
1419	Timbuktu Send Files (pre-5.2)	Logon is through UDP Port 407
1420	Timbuktu Exchange (pre-5.2)	Logon is through UDP Port 407
1443	WebSTAR/SSL Admin	WebSTAR port number plus 1000
3031	Program linking (Apple events)	Macintosh OS 9 and later
4000	Now public event server	
4199	EIMS Admin	
4347	LANsurveyor responders	Uses UDP also
5003	FileMaker Pro	Direct access, not through Web; UDP for host list
5190	AOL Instant Messenger	
5498	Hotline tracker	UDP port 5499 for finding servers
5500	Hotline server	
5501	Hotline server	
6699	Napster/Macster client	Used when server is in firewall mode
7070	Real Player	Also UDP ports 6970-7170
7648	CuSeeMe (video)	Client connections; UDP for audio/video
7649	CuSeeMe (video)	Connection establishment
19813	4D server	Previously 14566 (6.0 and earlier)

UDP port numbers

Port	Usage	Notes
53	DNS	Sometimes uses TCP
68	Dynamic Host Configuration Protocol (DHCP)	Commonly used to obtain a computer's IP address
69	Trivial File Transfer Protocol (TFTP)	
123	Network Time Protocol	
137	Windows Name Service	
138	Windows Datagram Service	
161	Simple Network Management Protocol (SNMP)	
407	Timbuktu	Handshaking only, prior to version 5.2
458	QuickTime TV	
497	Retrospect	Finding clients on the network
514	Syslog	
554	Real Time Streaming Protocol (QuickTime)	
2049	Network File System (NFS)	
3283	Apple Network Assistant	
5003	FileMaker Pro	For obtaining host list
6970 +	QuickTime and RealPlayer	
7070	RTSP alternate (RealPlayer)	

How do I create a new log file?

If your log file is becoming unwieldy due to its size, you may want to start over with a new log file. You do not have to delete the old log file, and can save it for record keeping.

If you do not disable logging before renaming or moving the log file, Norton Personal Firewall continues logging to that file until logging is disabled or the computer is restarted, after which the new file is created.

To create a new log file:

1. Double-click the **Norton Personal Firewall** icon or, on the Control Strip menu, click **Open Norton Personal Firewall** to start Norton Personal Firewall.
2. On the Edit menu, click **Preferences**.
3. Disable logging.
4. Rename the log file (called Norton Personal Firewall Log) or move it out of the Preferences folder.
5. Enable logging.

   Norton Personal Firewall will create a new log file in the Preferences folder.

Why doesn't Norton Personal Firewall load?

There may be an extension conflict if you have many extensions and virtual memory is turned off. Try enabling virtual memory or deleting unneeded extensions.

Why doesn't file sharing work?

You may have enabled file sharing over TCP/IP. By default, all TCP/IP services are initially protected from any access. You must specify access to file sharing before it will be accessible.

Questions about home networking

How do I protect all of the computers on my home network?

Install a copy of Norton Personal Firewall only on those computers with access to the Internet. If other computers are networked, but do not have Internet access, they do not need Norton Personal Firewall.

However, all computers connected to an Airport should have a copy of Norton Personal Firewall installed.

How do I specify access for a computer with a dynamically generated IP address?

Computers that get their IP address from DHCP (Dynamic Host Configuration Protocol) usually don't have the same IP address every time they connect to a network. However, their IP addresses usually fall within a given range. You can determine that range by checking the Access History window for denied accesses to that computer and noting the IP addresses used. You can then specify that range in the IP address list for the service for which you need to define access.

For information on checking the Access History window, see "To see the Access History window:" on page 50. For information on specifying a range of IP addresses for access, see "To add a range of addresses:" on page 58.

How does the firewall affect file and printer sharing?

Norton Personal Firewall provides security for TCP/IP connections. It does not affect AppleTalk connections. If you require that other computers have access to file sharing on your computer through TCP/IP, include their IP addresses in the allow access list for file sharing.

For information on allowing access to a service, see "Add IP addresses" on page 57.

3

Norton AntiVirus for Macintosh

CHAPTER 7

Protecting disks, files, and data from viruses

About automatic protection

You don't need to run Norton AntiVirus regularly as long as Auto-Protect is active. Auto-Protect interception prevents viruses from moving to your drive, and you can use the contextual menu to scan a specific volume, file, or folder. However, you do need to start the Norton AntiVirus application to set up a schedule for scanning or to change the preferences that were set during installation.

About Norton AntiVirus Auto-Protect

Norton AntiVirus Auto-Protect works independently of the Norton AntiVirus application. It loads on startup and alerts you if a virus is detected while you're working.

What part of my computer is protected?

Auto-Protect detects viruses within the SafeZones you choose in the General and SafeZone Preferences. Within designated SafeZones, Auto-Protect performs a virus scan on any file that is changed or created,

any file that is opened or launched, and any disks that are inserted. You can see and change what is protected, and where the SafeZones are through the general or custom preferences.

Turning Auto-Protect on or off with the Control Strip

Norton AntiVirus installs a Control Strip module so that you can turn Auto-Protect on or off without opening the Control Panel or the Norton AntiVirus application.

You must have the Control Strip Control Panel enabled.

To enable the Control Strip:

1. Click **Control Panels**.
2. Click **Control Strip**.
3. Make sure that Show Control Strip is selected, or that a Show/Hide Control Strip hot key is defined.

To turn Auto-Protect on or off from the Control Strip:

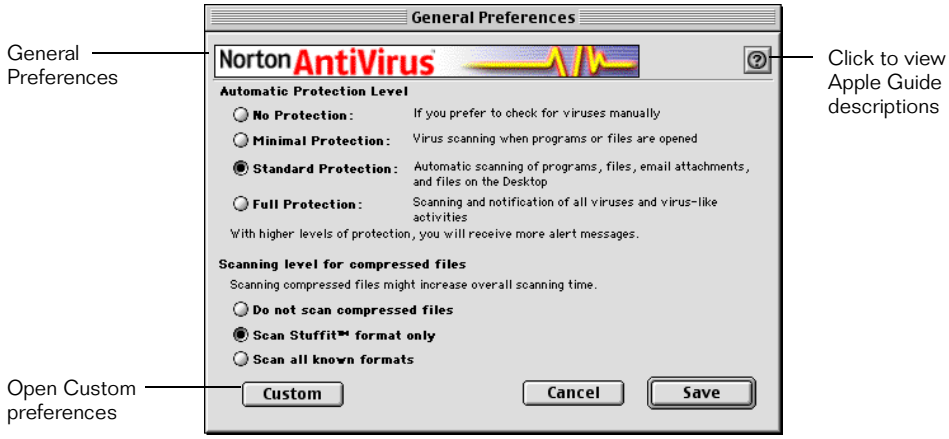
1. Click the Control Strip.
2. Click the Auto-Protect Control Strip module.
3. On the popup menu, do one of the following:
   - Click A**uto-Protect On**.
   - Click **Auto-Protect Off**.

Setting general and custom preferences

You can change the general settings that were set up when you installed Norton AntiVirus for Macintosh.

To set Norton AntiVirus preferences:

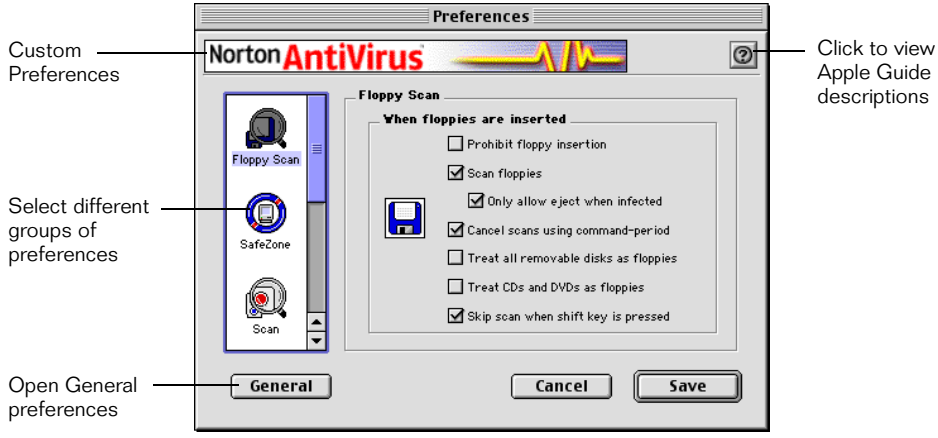
1 On the Preferences menu, click **General Preferences**.



2 Click a setting.

For descriptions of all of the settings, see the *Norton AntiVirus for Macintosh Reference Guide* on the CD.

3 To customize settings, click **Custom**.



4 Click an icon on the left to see the corresponding preferences.

Custom preferences take precedence over any protection level set in General preferences.

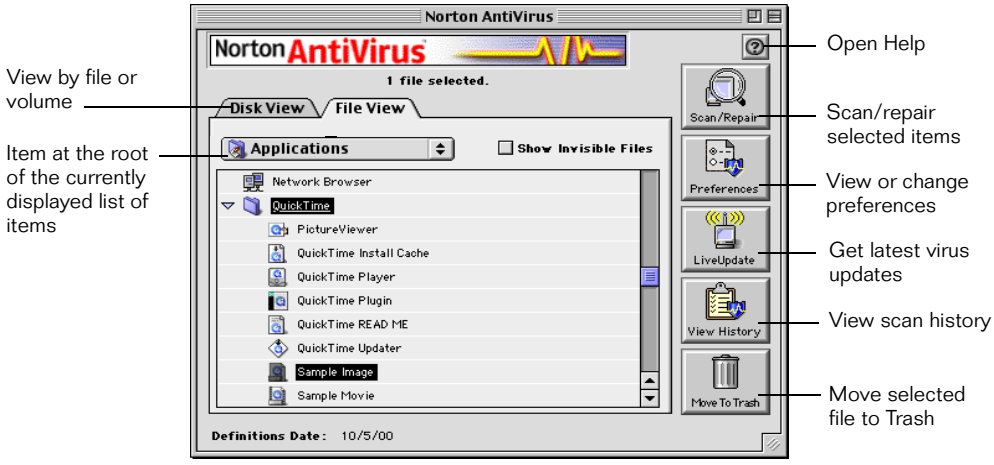
For detailed descriptions of the custom preferences, see the *Norton AntiVirus for Macintosh Reference Guide* PDF on the CD.

Scanning for viruses

When you install Norton AntiVirus, scan your hard disk as soon as you update your virus definitions. Perform full scans at regular intervals. This ensures that no undetected viruses have been transferred onto your hard disk.

Performing full scans is especially important if you do not have your automatic protection level set to Full Protection.

To have Norton AntiVirus scan a specific file, folder, or disk, drag its icon to the Norton AntiVirus program icon.



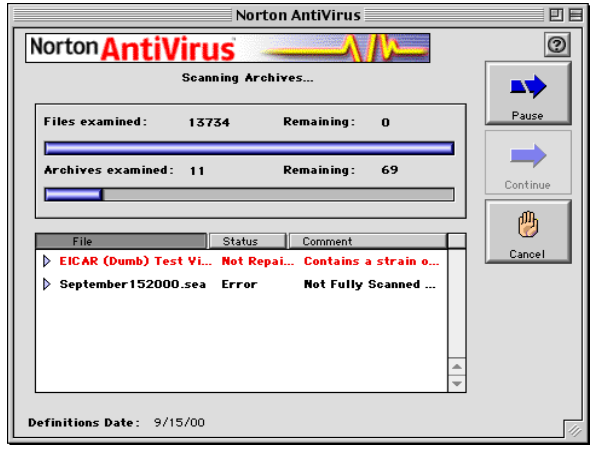
To start Norton AntiVirus and scan for viruses:

1 In the Norton AntiVirus folder, double-click **Norton AntiVirus**.

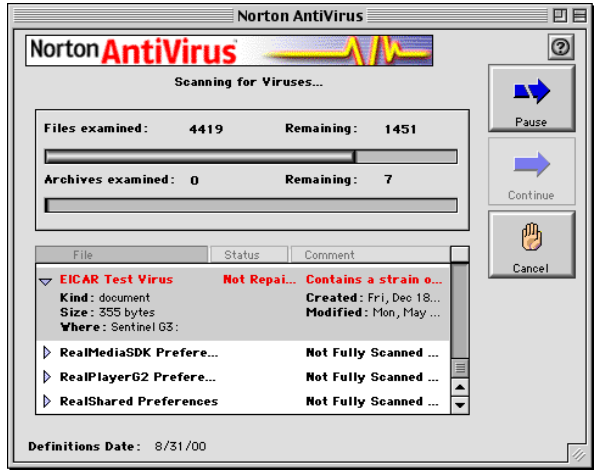
2 In the Norton AntiVirus main window, click a disk icon, folder, or file to scan.

3 Click **Scan** or **Scan/Repair**.

In the Finder, you can also use the contextual menu. For more information, see "Using contextual menus to scan" on page 80.



If a virus is found during the scan, Norton AntiVirus informs you.



4 Click **Done**.

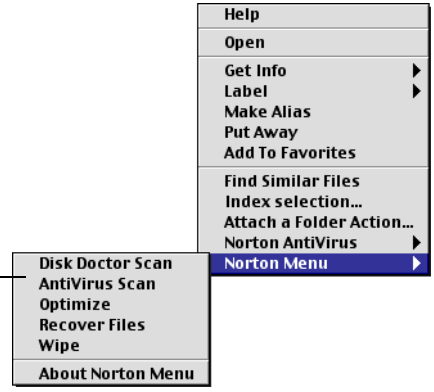
If Norton AntiVirus is configured to repair infected files automatically, the window informs you of this action. If it is not configured to repair automatically, or if it is a virus that Norton AntiVirus can't repair, you can take further action at the end of the scan. For details, see "If a virus is found while scanning" on page 89.

To exit Norton AntiVirus:

- On the File menu, click **Quit** or press **Command-Q**.

Using contextual menus to scan

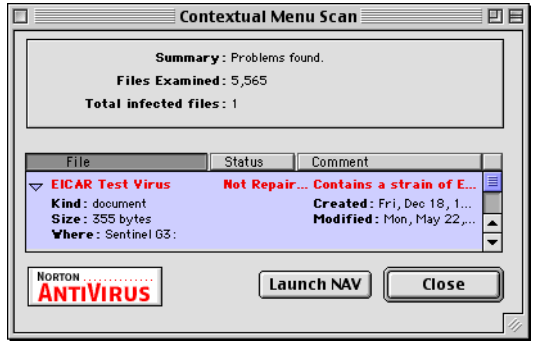
You can use the Macintosh OS contextual menu to scan a disk or item without starting Norton Internet Security.



Contextual menu lets you scan for viruses without starting Norton AntiVirus

To use the contextual menu:

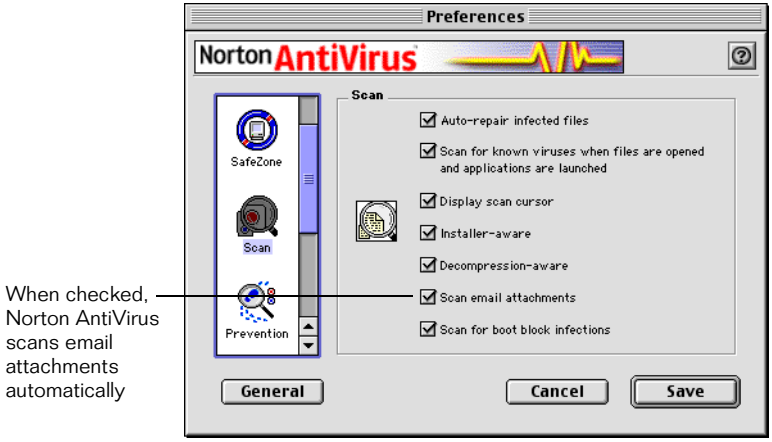
1. Press the Control key and click a disk, folder, or file icon, or anywhere on the Desktop.
2. On the contextual menu, click **Norton Menu > Virus Scan/Repair**.
3. The Small Scanner scans the selected item.



4. If you need to repair a virus, click **Launch NAV** to run the Norton AntiVirus main application.

Scanning email attachments

During installation, Norton AntiVirus searches for email client programs and identifies folders in which email attachments are saved. Norton AntiVirus adds these folders to its SafeZone list when any level of protection is active. All files that are saved in the email attachment folder are scanned automatically.



Scheduling automatic virus scans

To make virus prevention as easy as possible, Norton AntiVirus lets you schedule the following activities:

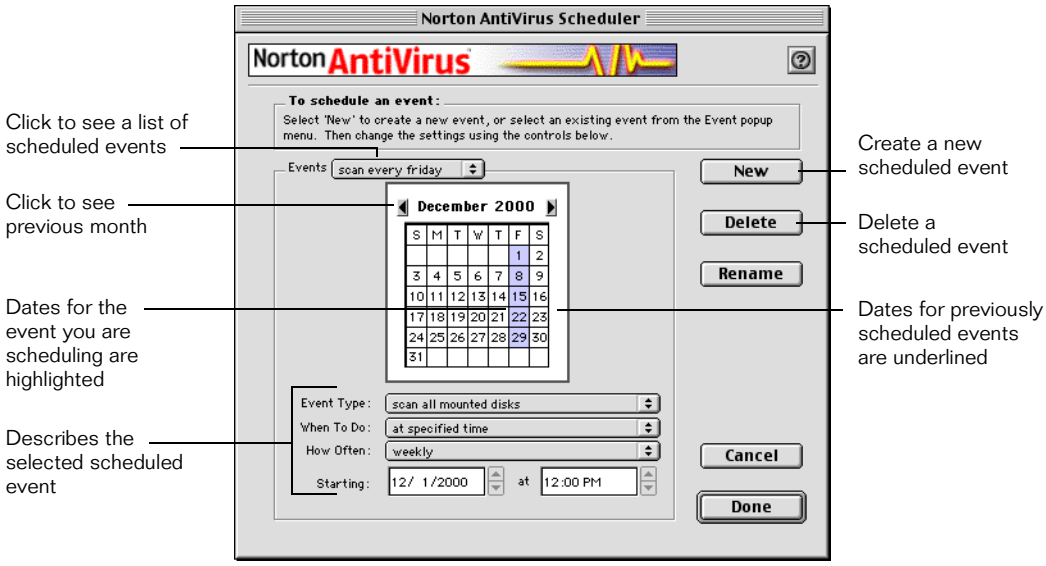
- Virus scans to occur at specified times. See "Scheduling a scan event" on page 82.
- Automatic updates of virus definitions with LiveUpdate. See "Scheduling LiveUpdate" on page 98.

If your computer is turned off during the time an event should take place, the event occurs the next time you start your computer.

For the best protection, schedule a LiveUpdate event to update your virus definitions, and then schedule a scan at a time after the latest virus definitions have been downloaded.

Scheduling a scan event

Follow the procedure below to schedule automatic virus scans.



To schedule virus scans:

1. On the Tools menu, click **Scheduler**.
2. Click **New**.

   A dialog box appears prompting you to type a name for the scheduled event.
3. Type the event name.
4. Click **OK**.
5. In the Event Type list, specify the item to scan.
6. In the When To Do list, specify when the scan should occur.
7. In the How Often list, specify the frequency of the scan.

   The days on which the scans will occur are highlighted in the calendar.
8. In the Starting date and time text boxes, select the correct time and date information.

   The Minute option is dimmed if the scan occurs at startup or shutdown.
9. Click **Done**.

To schedule virus definitions and program updates, use the LiveUpdate Scheduler. For more information, see "Scheduling LiveUpdate" on page 98.

Editing and deleting scheduled events

You can make changes to events that you schedule. For a description of the scheduling options, see "Scheduling automatic virus scans" on page 81.

To edit a scheduled event:

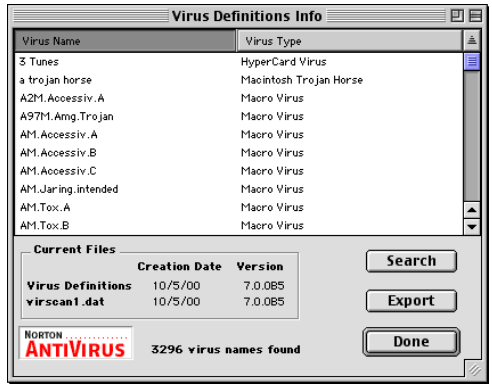
1. On the Tools menu, click **Scheduler**.
2. In the Event list, click the scheduled event to change.
3. Make your changes by selecting different schedule options.
4. To change the event name, click **Rename** and type a new name.
5. Click **Done**.

To delete a scheduled event:

1. On the Tools menu, click **Scheduler**.
2. In the Event list, click the scheduled event to delete.
3. Click **Delete**.
4. Click **OK**.
5. Click **Done**.

Looking up virus names and definitions

You can look up a virus name from within the Norton AntiVirus application. The Virus Definitions Info dialog box lists all of the viruses in the current virus definitions file. You can export this list to print it in your word processing program.



To make sure that you have the latest virus definitions, run LiveUpdate. For more information, see "Keeping virus definitions and program files current" on page 93.

To view virus names:

1. On the Tools menu, click View Virus Definitions Info.
2. In the Virus Definitions Info dialog box, do one of the following:
   - Click **Export** to export the virus list to a text file, and specify where to save the file. Open the exported text file in a word processing program to print it.
   - Click **Search** to search for a specific virus name. In the Virus Name Contains field, type the name or part of the name and click Find.

Because of the large number of viruses, the Virus Definitions Info file does not include descriptions of each virus. The Symantec AntiVirus Research Center Web site contains a list of all known viruses and related malicious code, along with descriptions.

Looking up virus definitions on the Symantec Web site

You can view descriptions of different Macintosh system viruses in the Virus Encyclopedia on the Symantec AntiVirus Research Center Web site.

To view the latest virus descriptions:

1. Point your browser to the following Web site:

   http://www.sarc.com/
2. Click the link to the Virus Encyclopedia.
3. Type a virus name to search, or scroll through the alphabetical list to locate a virus.
4. Click a virus to read its description.

Fine-tuning Auto-Protect performance

If you choose the highest level of automatic protection, you might notice that your computer's performance is affected during some activities.

If you have Norton Utilities for Macintosh installed on your system, the FileSaver Control Panel, combined with Norton AntiVirus Auto-Protect, generates activities that might cause performance impairment if you have set maximum protection for each program. Both FileSaver and Auto-Protect scan your disk and keep track of current and deleted files.

You have a variety of options for fine-tuning the protection activity. Before making adjustments, try to determine the activity that seems to cause performance impairment, and make adjustments related to that activity.

If you notice a decrease in your computer's performance, lower the levels of protection for Auto-Protect, and the level of scanning for FileSaver.

To minimize protection levels in Norton AntiVirus:

- In the General Preferences dialog box, lower the protection level by doing the following:
  - Under Automatic protection level, click **Minimal Protection** or **No Protection**.
  - Under Scanning level for compressed files, click **Do not scan compressed files**.
- In the Custom Preferences dialog box, lower the protection level in each area doing the following:

- Prevention preferences: Turn off the setting that monitors virus-like activities.
- Scan preferences: Turn off automatic scanning of files when opened and programs when launched.
- Compression preferences: Limit the number of file types that are scanned.
- SafeZones: Limit the number of SafeZones by clicking **Disable SafeZones**, or click **Custom** and limit the selected SafeZones protected by Auto-Protect.

To minimize protection levels in FileSaver:

1. In the FileSaver control panel, for the selected disks, uncheck settings for **Track Deleted Files/Folders**.
2. On the Update Schedule tab, minimize the frequency of updates.

CHAPTER 8

Responding to virus alerts

About virus alerts

Auto-Protect alerts you to virus and virus-like activity, whether the infected file is repaired automatically or not. If you have a higher level of protection, you might receive a higher number of alerts.

For information on minimizing the number of alerts, see "Setting general and custom preferences" on page 77.

When Auto-Protect finds a virus

If Auto-Protect finds a virus but does not (or cannot) repair it

Look for words that identify the type of problem. Read the entire message.

- Click the button of the action you want to take.

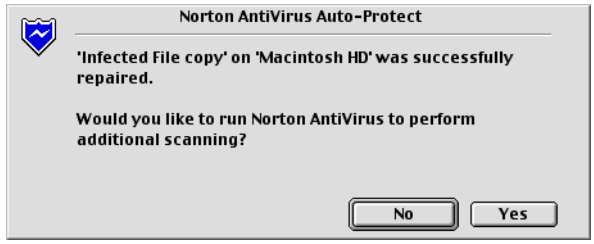
Repairing the infected file is always the best choice. It eliminates the virus and repairs the infected item automatically.

For more information, see "What to do if a virus is found" in the *Norton AntiVirus for Macintosh Reference Guide* on the Norton AntiVirus CD.

If Auto-Protect finds a virus and repairs it

When Norton AntiVirus Auto-Protect reports that it repaired an infected file, you don't have to do anything.

A message informs you when an infected file is repaired.



Even when Auto-Protect has repaired the infected file, ensure that no other viruses exist on your computer by running Norton AntiVirus.

If a floppy is infected and ejected

When Standard Protection is set, Auto-Protect will eject infected floppy disks. You can bypass this setting by holding down the Shift key while inserting the floppy disk.

If you want to repair the infected floppy disk, use Norton AntiVirus to scan and repair it.

To repair an infected floppy disk:

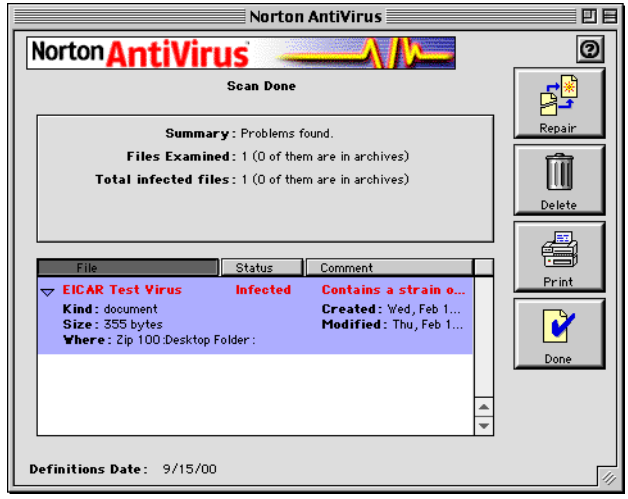
1. Start Norton AntiVirus.
2. Insert the floppy disk while holding down the Shift key on your keyboard.
3. In the Norton AntiVirus main window, select the floppy disk to scan.
4. Click **Scan** or **Scan/Repair**, and follow the instructions for "If a virus is found while scanning", below.

If a virus is found while scanning

If you are scanning with Norton AntiVirus and a virus is found, Norton AntiVirus repairs it, unless you changed the default settings. If an infected file is discovered, the file is listed as infected in the scan window.

If an infected file appears in the scan window:

1. Click the infected file in the scan results window.
2. Click the triangle to the left of the file to view more information about the file.



   The status will be Repaired or Not Repaired.
3. If a selected file can't be repaired, click **Delete**.

If Norton AntiVirus can't repair a file

Sometimes viruses damage files beyond repair. If Norton AntiVirus finds an irreparably damaged file, you must delete the infected file and replace it with an uninfected backup copy.

Make sure that you have scanned with the latest virus definitions. If you are not sure that you have the latest virus definitions, use LiveUpdate. See "Keeping virus definitions and program files current" on page 93 for details.

To delete an infected file:

1. Run Norton AntiVirus and scan the infected file.

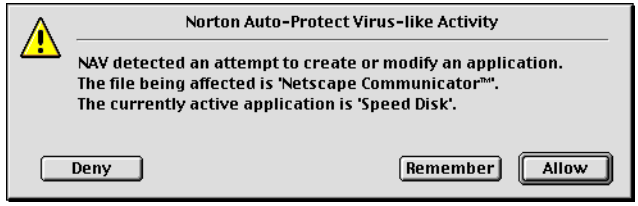
   In the scan window, the file will indicate that it is Repaired or Not Repaired.
2. In the scan window, click the infected file.
3. Click **Repair**.
4. If a file can't be repaired, click **Delete**.
5. Click **OK**.

   The Status column shows that the file is Deleted.

If a Virus-like Activity alert appears

A Virus-like Activity alert is a warning and does not necessarily mean that your computer has a virus. You can decide whether the operation is valid, for example, when you are installing software or decompressing a compressed archive.

You can set the types of virus-like activities checked.



To respond to a Virus-like Activity alert:

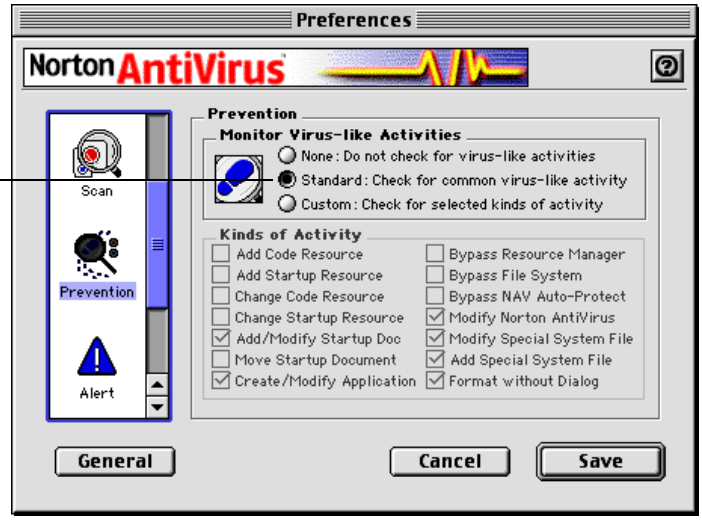
1. Do one of the following:
   - Click **Remember** if you don't want the alert to appear when this activity occurs again.
   - Click **Allow** if the message describes a valid activity for the application you are running.

     For example, if you are changing a system setting, or making a copy of an application or system file, you can let the activity continue.
   - Click **Deny** if the detected activity isn't related to what you are trying to do.

   Depending on the activity, Auto-Protect displays different responses.

2 Press **Return** to choose the recommended action for the situation.

See the Prevention Preferences to specify the Virus-like Activities that are monitored.



Select a monitoring level for Virus-like Activities

For full descriptions of virus-like activities, see the *Norton AntiVirus for Macintosh Reference Guide* PDF on the CD.

APPENDIX A

Keeping virus definitions and program files current

LiveUpdate can be used to keep your virus definitions files and program files updated. If you have an Internet connection, LiveUpdate is the most efficient method to update your files.

If you use America Online (AOL) as your Internet Service Provider (ISP), you must log on to AOL before you use LiveUpdate. For more information, see "Using LiveUpdate with America Online" on page 102.

About LiveUpdate

Symantec provides online access to updated program files with your subscription.

Using your existing Internet connection, LiveUpdate connects to the Symantec LiveUpdate server, checks for available program updates, then downloads and installs them.

If you have Norton Internet Security for Macintosh installed, LiveUpdate also updates virus definitions files and Norton Internet Security program files, as well as its own program files.

How to update virus protection

Use LiveUpdate to download and install the latest virus definitions and program update files with your subscription.

Virus definitions files are also available on the Symantec Web server, at the Symantec Web site:

http://www.sarc.com

For information about these and other methods, see "Service and support solutions" on page 103.

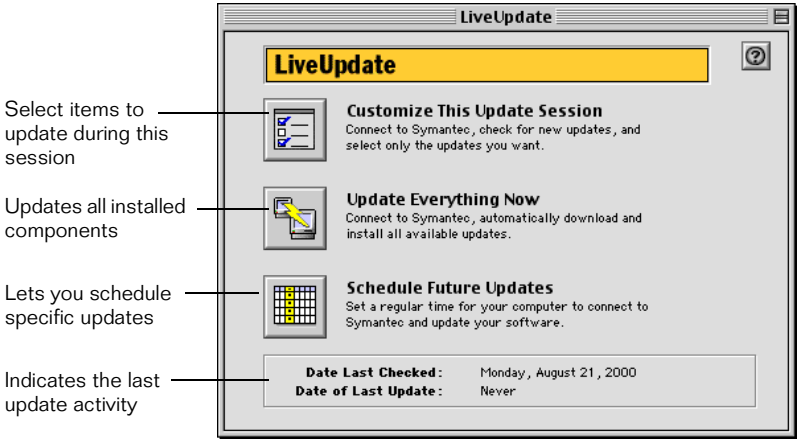
When to update virus protection

Run LiveUpdate as soon as you have installed Norton Internet Security. Once you know that your virus definitions and program files are completely up-to-date, run LiveUpdate at least once a month.

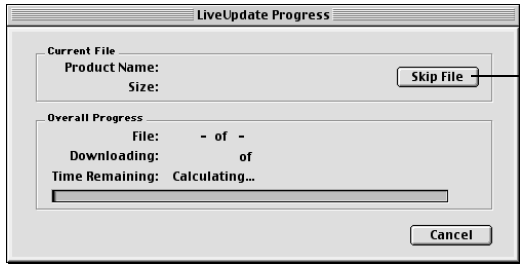
New virus definitions files are made available monthly with your subscription. You can run LiveUpdate manually, or use the LiveUpdate scheduler. For more information, see "Scheduling LiveUpdate" on page 98.

Updating virus protection and program files

You can have LiveUpdate look for updates to all files at once, customize your update selection, or schedule a future LiveUpdate session.

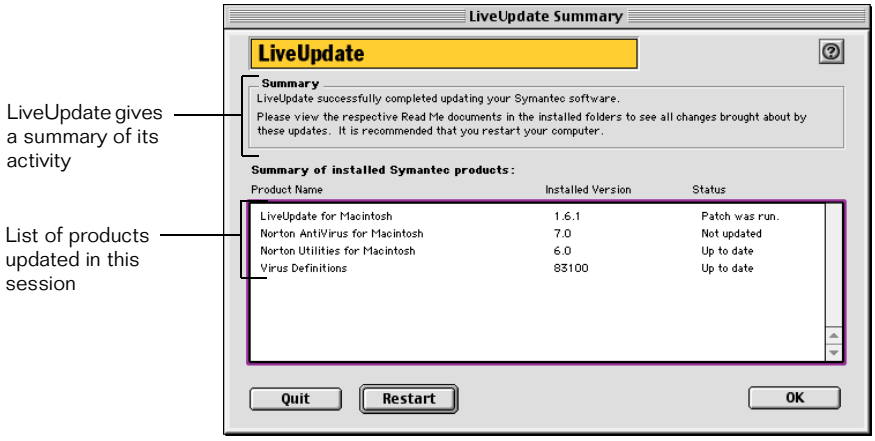


LiveUpdate downloads and installs the available updates. A status dialog box keeps you informed of the file transfer process.



The file transfer takes a few minutes. When the file transfer is complete, LiveUpdate notifies you.

If your files are up-to-date, LiveUpdate informs you.



To update virus definitions and program files with LiveUpdate:

1. In the Norton Internet Security folder, click **LiveUpdate**.
2. Do one of the following:
   - To update all files, click **Update Everything Now**.
   - To specify what to update during the current session, click **Customize This Update Session**.

     For more information, see "To customize a LiveUpdate session:" on page 97.

- To open the LiveUpdate Scheduler and schedule LiveUpdate events, click **Schedule Future Updates**.

  For more information, see "To schedule a LiveUpdate event:" on page 98.

3. Click **Close**.
4. If LiveUpdate tells you that you need to restart your computer, click **Restart**.
5. On the File menu, click **Quit**.

Emptying the Trash after a LiveUpdate session

After you update program files with LiveUpdate, there are items in the Trash. LiveUpdate moves the older discarded files to the Trash. Empty the Trash. If you haven't already restarted after installing the application, you might get a message that these files are in use. After you restart your computer, you can empty the Trash.

Reading the LiveUpdate What's New file

LiveUpdate places a What's New file on the Desktop. This contains details of what files were updated by LiveUpdate.

To read the What's New file:

- Double-click the file to read about the contents of the updated files.

  The file opens in SimpleText.

To close the What's New file:

- Press **Command-Q** to quit SimpleText.

To delete the What's New file:

- Drag it to the Trash.

Checking version numbers and dates

LiveUpdate lets you know if your program files and virus definitions are up-to-date by displaying the version numbers and the status. The Norton AntiVirus main window displays the date of the most recently installed product. You can also check the program file and virus definitions in the application's About box, accessible from the Apple menu.

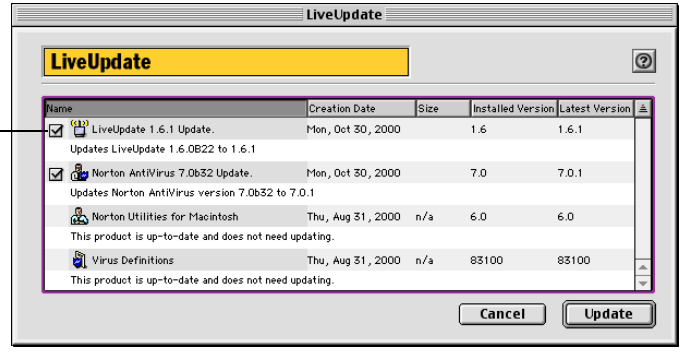
To view an application's About box:

1. Start Norton Internet Security.
2. On the Apple menu, click **About Norton Internet Security**.

   The About box lists version number and copyright dates.
3. When you've finished viewing the About box, click **OK**.

Customizing a LiveUpdate session

LiveUpdate lets you update only one or two items and omit the items you don't want to update.



Select items to update during the current session

To customize a LiveUpdate session:

1. In the LiveUpdate window, click **Customize This Update Session**.

   LiveUpdate scans your disk to see what applications are installed, and presents a list of available updates.
2. Check items to update in this session.

   LiveUpdate will not look for items that are unchecked. If your files are already up-to-date, no items are selectable.
3. Click **Update**.

   The file transfer takes a few minutes. When file transfer is complete, LiveUpdate notifies you.

   If your files are up-to-date, LiveUpdate informs you.

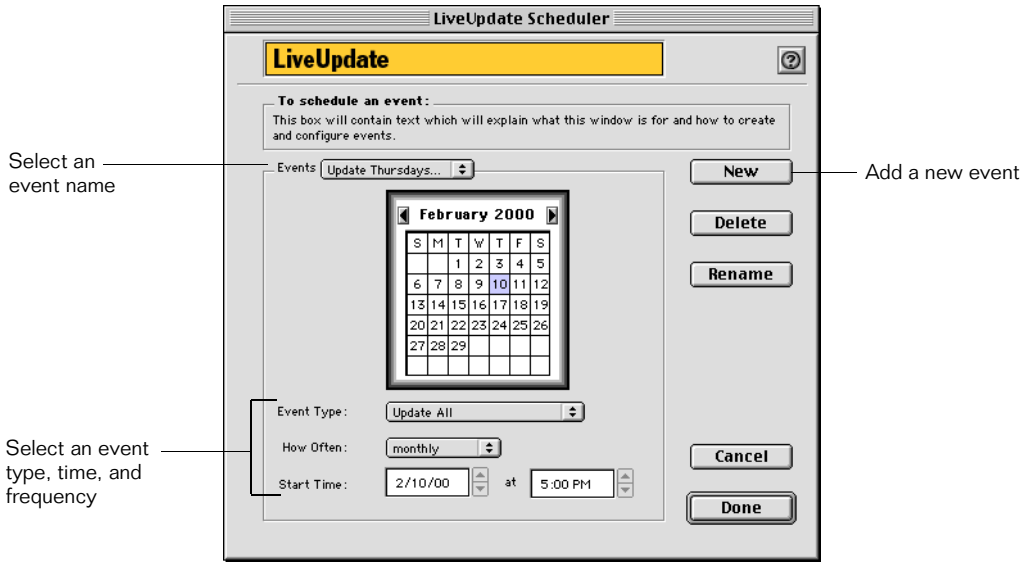
Scheduling LiveUpdate

You can schedule automatic LiveUpdate sessions to update program files and virus protection. Using the LiveUpdate Scheduler, you can set up events to run automatically.

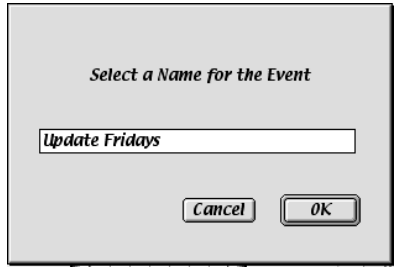
Before scheduling automatic virus protection updates, make sure the update process works correctly by stepping through the process manually. See "How to update virus protection" on page 93 for instructions.

To schedule a LiveUpdate event:

1 In the LiveUpdate main window, click **Schedule Future Updates**.



2 In the LiveUpdate Scheduler dialog box, click **New**.



3 Type the event name.

4 Click **OK**.

5 Specify the Event Type, How Often, and the Start Time of updates.

Updated virus definitions files are posted on the Symantec LiveUpdate server and Web site around the first of every month, or more frequently when necessary.

The days on which updates occur are highlighted in the calendar. Dates for other scheduled events are underlined.

6 Finish scheduling the update by typing the schedule time and date.

- Click the **Hour** text box and use the arrow keys to set the start hour.
- Click the **Minute** text box to set the start minute.

Your computer must be turned on for LiveUpdate to run at the scheduled time. If your computer is not on at the scheduled time, LiveUpdate starts the next time you start your computer.

7 Click **Done**.

Updating virus definitions from other sources

When a new virus definitions file becomes available, Symantec posts messages on the Symantec Web site. If you can't run LiveUpdate, you can download new virus definitions files from the Symantec Web site.

Downloading files from the Symantec Web site

The latest virus definitions files are posted regularly on the Symantec Web site.

To download files from the Symantec Web site:

1 Open your Internet browser and go to the following site:

http://www.sarc.com/avcenter/defs.download.html

If this page doesn't load, go to http://www.sarc.com and click the **Download Virus Definition Updates** link.

2 On the Download Virus Definitions page, select **Norton Internet Security for Macintosh**, along with your preferred language.

3 Click **Download Updates**.

4 On the Download Updates page, click the file to download.

Be sure to click files for the appropriate version of Norton Internet Security for Macintosh (Version 7).

Information about the update is included with the download and a text file describes how to install the update.

Deleting the NAV™ 7.0 QuickScan file

Because of the way Norton Internet Security tracks scanned files, a new virus already present on your hard drive could go undetected when you first update definitions—even though those definitions would detect any new files with that virus.

If you have scanned your hard disk and found no viruses, and then you download new virus definitions, you might want to ensure that any previously undetected viruses will be found by the new definitions.

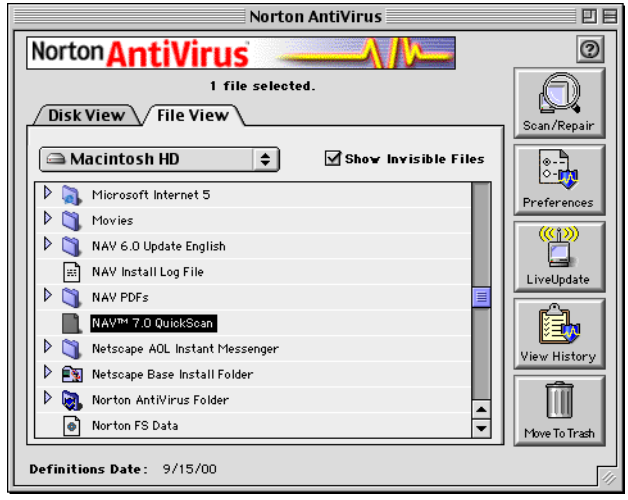
You can use Norton Internet Security to delete the file at the root of each drive called NAV™ 7.0 QuickScan.

To remove the QuickScan file:

1 In the Norton AntiVirus window, click the **File View** tab.

2 In the File View list, double-click your hard disk and locate the NAV 7.0 QuickScan file.

Ensure that **Show Invisible Files** is checked.



3 Click the **NAV™ 7.0 QuickScan** file.

If there are other QuickScan files left over from previous versions of Norton AntiVirus, select them as well.

4 Click **Move To Trash**.

5 Click **OK**.

6 Click anywhere on your Desktop.

7 On the Special menu, click **Empty Trash**.

After deleting this file, the first scan with the new virus definitions will be slower, but will detect any previously undetected viruses.

Downloading updates from the Symantec Web site

The latest virus definitions files are posted regularly on the Symantec Web site.

To download files from the Symantec Web site:

1 Start your Internet browser and go to the following site:

http://www.sarc.com/avcenter/defs.download.html

If this page doesn't load, go to http://www.sarc.com and click the **Download Virus Definition Updates** link.

2 On the Download Virus Definitions page, click **Norton Internet Security for Macintosh**, along with your preferred language.

3 Click **Download Updates**.

4 On the Download Updates page, click the file to download.

Be sure to click files for the Norton Internet Security for Macintosh Version 7.

Information about the update is included with the download and a text file describes how to install the update.

Using LiveUpdate with America Online

If you use America Online (AOL) as your Internet Service Provider (ISP), you might need to log on to AOL before you use LiveUpdate.

To use LiveUpdate with AOL:

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Start LiveUpdate.
4. Follow the procedure from "To update virus definitions and program files with LiveUpdate:" on page 95.
5. When the LiveUpdate session is complete, quit AOL.

   If your LiveUpdate session requires that you restart your computer, disconnect from AOL before restarting.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index. Macintosh users can click the About... command on the Apple menu, and then click Info to view Technical Support and Customer Service contact information.

Technical support

Symantec offers several technical support options:

- StandardCare support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, then select your product and version. This gives you access to product knowledge bases, interactive troubleshooter, Frequently Asked Questions (FAQ), and more.

- PriorityCare, GoldCare, and PlatinumCare support

  Fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

  For telephone support information, connect to http://service.symantec.com, select your product and version, and click Contact Customer Support.

- Automated fax retrieval

  Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 984-2490.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for six months after the release of the new version. Technical information may still be available through the Service & Support Web site (http://service.symantec.com).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Visit Symantec Customer Service online at http://service.symantec.com for assistance with non-technical questions and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at: http://www.symantec.com/upgrades/ or call the Customer Service Order Desk at (800) 568-9501.

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://www.symantec.com, select the country you want information about, and click Go!

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

Argentina, Chile, and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.symantec.com/region/mx
+54 (11) 4315-0889
Fax: +54 (11) 4314-3434

Asia/Pacific Rim

Symantec Australia Pty. Ltd.
408 Victoria Road
Gladesville, NSW 2111
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 9850 1000
Fax: +61 (2) 9817 4550

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.symantec.com/region/br/
+55 (11) 3048-7515
Fax: +55 (11) 3048-7510

Colombia, Venezuela, the Caribbean, and Latin America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/region/mx/
+1 (541) 334-6054 (U.S.A.)
Fax: (541) 984-8020 (U.S.A.)

Europe, Middle East, and Africa

Symantec Customer Service Center P.O. Box 5689 Dublin 15 Ireland	http://www.symantec.com/region/reg_eu/ +353 (1) 811 8032 Fax: +353 (1) 811 8033
Automated Fax Retrieval	+31 (71) 408-3782

Mexico

Symantec Mexico Blvd Adolfo Ruiz Cortines, No. 3642 Piso 14 Col. Jardines del Pedregal Ciudad de México, D.F. C.P. 01900 México	http://www.symantec.com/region/mx +52 (5) 661-6120

Virus protection subscription policy

If your Symantec product includes virus protection, you might be entitled to receive free virus protection updates via LiveUpdate. The length of the free subscription could vary by Symantec product.

When you near the end of your virus protection subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your free subscription ends, you must renew your subscription before you can update your virus protection. Renewal subscriptions are available for a nominal charge.

To order a subscription, do one of the following:

- Visit our Web site at: http://www.shop.symantec.com.
- Outside the United States, contact your local Symantec office or representative.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

October 2000

Norton Internet Security for Macintosh
CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name _____

Company Name _____

Street Address (No P.O. Boxes, Please)_____

City _____ State _____ Zip/Postal Code _____

Country* _____Daytime Phone _____

Software Purchase Date _____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

Briefly describe the problem:_____

_____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	_____
Shipping & Handling	$ 4.95
TOTAL DUE	_____

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _____ __ Visa __ Mastercard __ American Express

Credit Card Number _____Expires _____

Name on Card (please print) _____ Signature _____

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234

Please allow 2-3 weeks for delivery within the U.S.

SYMANTEC.™

G L O S S A R Y

The first use of the following terms in the Norton Personal Firewall section of the book is indicated in the text in *italic*.

AppleTalk — Protocol used by some network devices, such as printers and servers, to communicate.

connection-based protocol — A protocol that requires a connection before information packets are transmitted.

connectionless protocol — A protocol that sends a transmission to a destination address on a network without establishing a connection.

DHCP — Dynamic Host Configuration Protocol. DHCP dynamically assigns IP addresses to devices on a network.

Domain Name System (DNS) — Service that translates host names into IP addresses.

firewall — Filter that blocks or allows connections and data transmission over the Internet.

FTP — File Transfer Protocol. An application protocol used for transferring files between computers.

hacker — A person who attempts unauthorized access of other people's computers for the purpose of obtaining information on those computers or to do damage to those computers.

host name — The name that identifies a computer on a network. For example, www.symantec.com is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS.

Internet — A decentralized global network connecting millions of computers.

Internet protocol (IP) address — Number that uniquely identifies your computer on the Internet.

PPP — Point-to-Point Protocol. A method of connecting to the Internet that provides error-checking features.

protocol	Set of rules governing the communication and transfer of data between computers. Examples of protocols are HTTP and FTP.
proxy server	A server that attempts to fulfill requests between a client and another server to which the request was directed. If it cannot, it forwards the request to the real server. Proxy servers are used to speed access to the Web and to filter requests to the Web.
subnet	A local area network that is part of a larger intranet or the Internet.
subnet mask	A code, in the form of an IP address, that computers use to determine how much of an IP address identifies the subnet and how much identifies an individual computer on that subnet.
TCP/IP	Transmission Control Protocol/Internet Protocol. Common name for the protocols developed by the US Department of Defense to support the construction of worldwide networks. TCP is used to check and correct transmission errors; IP is used for data transmission.
Trojan horse	Program masquerading as something desirable, such as a legitimate software program, that does something unexpected in reaction to a trigger event.
UDP	User Datagram Protocol. A simple protocol used to exchange information without acknowledgment or guaranteed delivery.
virus	Small program designed to replicate and spread, generally without the user's knowledge.
Web server	A computer containing server software that sends requested Web pages to your browser.

I N D E X

D

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W

Z